**Individual Report**

**Member name:Justin Young**

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

**Date: 09/04/2023**

**Tasks Assigned:**

* Come up with questions related to the project's main topic and supporting research papers.
* Literature review of research papers.
* In-depth report of one research paper found (Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning).
* Preparing Gantt chart.
* Evaluate Sangeeth Santhosh’s individual in-depth report and individual progress report.

**Summary:**

* In-depth report created on ‘Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning’
* This study’s objective is to demonstrate systems and methods to ensure ML-based security in mobile applications
* The “Behavior Approach” procedure along with ML methods KNN, Naive Bayes and Decision trees are used to determine their effectiveness
* Study is done on an Android phone, as it is the most popular mobile operating system by a significant margin and has greater security risk as the system is open source
* Research provides 4 steps (Start, Show, Ignore and Hide) to begin enacting the system
* For this study, the system is implemented with the mentioned ML methods and supported by the “Derbin” dataset in Py-charm.
* Additionally, images displaying what the system looks like in use are also provided
* ML methods are implemented in the system with the resulting accuracy measurements:
  + KNN - 91.99%
  + Naive Bayes - 97.37%
  + Decision trees - 89.98%
* Major conclusions drawn from this paper include “feature matching” as a weak point for ML models, and the Naive Bayes method was most effective in detecting malicious behavior on mobile devices.

**Outcome:**

This paper provides a point of focus (feature matching) when designing an ML-based system in mobile devices, a system guideline that can be followed for implementation (Behavior’s Approach) and a resulting most effective ML method (Naive Bayes) from the study conducted

**References** *(with citation)*

[34] S. Vanjire and M. Lakshmi, “Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning, in *2021 International Conference on Artificial Intelligence and Machine Vision*, Gandhinagar, India, pp. 1-4, doi: 10.1109/AIMV53313.2021.9671009

**Evaluation of Report  
  
Evaluation by:** [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu) **Date: 09/04/2023**

**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]**

* Each important element in the individual progress report has been examined in detail.

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

* Yes, Each section of the guidelines has been completed to an adequate level.

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

* The quality of this version of the written report is satisfactory since it adequately covers the required duties, provides a summary, and provides an analysis of the results. **Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 09/04/2023**