**Individual In-depth Report**

**Member name:** [Justin Young](mailto:jtyoun15@asu.edu)

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

**Date:** 09/03/2023

**Tasks Assigned:**

* Literature review of Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning.

**Summary:**

* The overall purpose of this paper is to demonstrate behavior-based machine learning (ML) methods to ensure security for mobile devices.
* Methods used are KNN, Naive Bayes and decision trees (tested on an Android phone, as it is the most popular within the mobile phone industry and is open source, which allows for greater security risks)
* Two types of malware detection are identified (Static and dynamic detection), and concludes that dynamic detection is more effective due to the sophistication of modern malware on Android devices
* States that one point of struggle for ML models is feature matching (seen more commonly in sophisticated attacks)
* 4 steps are given in the designing process to begin detecting activity on applications
  + Start (starting the application, monitoring the system
  + Show (displaying application usage)
  + Ignore (display ignored applications
  + Hide (display hidden or background applications)
* To demonstrate previously mentioned ML methods, they are used in a system implemented with the “Derbin” dataset in Py-charm, the accuracy of each method is recorded.
* Results of the study:
  + Naive Bayes (97.37%)
  + KNN (91.99%)
  + Decision Tree (89.98%)
* Research concludes that feature matching is still a point of struggle in ML systems, but rigid frameworks and implementation of the studied systems can combat that weak point.

**Outcome:**

This study helps in identifying a system and supporting ML methods to help ensure security in mobile devices, and provides resulting data from the study showing the accuracy of the tested methods. In this study, the Naive Bayes theorem proved to be the most effective method with 97.37% accuracy.

**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 summary with justification.**

The paper provides a valuable evaluation of behavior-based ML methods for mobile device security, using KNN, Naive Bayes, and decision trees. The study's structured approach and testing on an Android device make it a credible resource for evaluating these techniques.

**The quality of the major result(s) with justification.**  
The study's major result is the performance evaluation of ML methods, with Naive Bayes achieving the highest accuracy (97.37%). This result is robust and supports the paper's argument for using behavior-based ML for mobile security.

**The usefulness of the paper to the overall project.**   
The paper is relevant to the project, offering insights into the practical application of ML techniques aligning with project's objectives.

**Other comments**

None

**Evaluation Approval  
  
Evaluation by:** [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu) **Date:** 09/03/2023

**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

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

* Yes

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

* Yes

**Approval.  
  
Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date:** 09/04/2023 **Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

Yes, the quality of this written in-depth study report and evaluation report is satisfactory.