EGCI491: Assignment II

Enter your name here

January 30, 2026

Chapter 2
Literature Review

Provide a brief description of what this chapter covers. It is typically an outline of a comprehensive literature review for the whole project. All related papers and previous works should be reviewed. You should summarize the main contributions, techniques used, data, key findings, and research gaps of each paper.

2.1 Comparison of Deep Learning and the Classical Machine Learning Algorithm for the Malware Detection [1]

This paper proposed a malware-detection comparison between using Deep Neuron Network (DNN) and using Randon Forest (RF).

Four different feature sets of Malicia data are used for performance evaluation.

True positive Rate (TPR), True negative Rate (TNR), and Positive Predictive Value (PPV), including Precision and Accuracy (Acc.) were caculated and used for performance comparison.

The experiment indicated that RF performs better that DNN. This may be due to the combination of Auto-Endocoders used for feature extraction and DNN used for feature classification , which is too complex to predict malware using opcode frequency as a feature.

The future work is the investigaion of using other machine learning techniques such as RNN, LSTM, and ESN with more advanced feature extraction approaches.

2.2 Android Malware Detection Using Static Features and Machine Learning [2]

This paper proposed a static feature-based machine learning approach for android malware detection.

A combinatoon of various static features such as opcode, permissions, and API calls of Android Application Pakage (APK) were used and compared with using a single type of APK.

Several machine lerning technies included Linear Classifier, oosted Trees, Gaussian Naive Bayes, Decision Tree, Random Fores (RF), and Support Vector Machine (SVM) were used for malware detection and comparison.

In this work, data set used were collected from 1) Andriod Malware Dataset (AMD), 2) Kuafu Det Dataset, and Omnidroid Dataset were used. 60% of them were used for training, and the remaning is for performance testing in terms of True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN).

The experiment showed that Gaussin Process, RF, and Decision Tress provided the most promissing results, respectively.

The future work is to apply dynamic feature extracted from APK files to filter out clssiified malware as benign. In addtion, more advanced machine learning methods such as Deep Neuron Network will also be used with better feature selection approaches to excluse redundant and unnecessary featurwes .

Reference

[1] Mohit Sewak, Sanjay K. Sahay, and Hemant Rathore. Comparison of deep learning and the classical machine learning algorithm for the malware detection. *2018 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pages 293–296, 2018. doi: 10.1109/SNPD.2018.8441123.

[2] Ali Al Zaabi and Djedjiga Mouheb. Android malware detection using static features and machine learning. *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, page 1–5, 2020. doi: 10.1109/CCCI49893.2020.9256450.