ABSTRACT

This study investigates the application of the Deep Neural Decision Forest (DNDF) technique for identifying obfuscated malware, focusing on enhancing the deep neural network model and decision forest algoritm. Utilizing 10-fold crossvalidation, the research confirms the model's resilience to data variance and equilibrium. Incorporating Extra Trees in the training phase aids in pinpointing pertinent features, thereby elevating the precision of detection, notably in imbalanced datasets. The study advances the field of obfuscated malware detection by employing a DNDF strategy and a comprehensive evaluation methodology. The findings of this study are anticipated to significantly bolster system defenses against increasingly sophisticated malware attacks. In the binary class classification test, the model achieved an exceptional accuracy rate of 99.8%, with the precision, F1-Score, and recall recorded at 99.83%, 99.8%, and 99.77% in that order. The model processed each instance of training data with an average efficiency of 99.4962 seconds. When applied to 4-class classification, the model showcased notable efficacy, achieving an accuracy of 72.64%, precision and recall rates of 79.35% and 72.64% respectively, and an F1- Score of 67.85%. Even with heightened complexity, the model maintained its efficiency in data training sessions, averaging 110.5303 seconds. The evaluation utilized the CIC-MalMem-2022 dataset, solidifying the system's validity as an effective malware detection tool in practical environments.

Key Word: Malware detection, obfuscated malware, Neural Decision Forest, feature selection, Extra Trees Classifier.