Machine Learning Approaches to Classify Malware Data

Sabah Iqbal, Shiemaa Adlan
Security Analyst at Pure Health group

Abstract

With the recent increase in the use of the Internet, there has been a rise in Malware attacks. Malware attacks can lead to stealing confidential data or make the target a source of further attacks. The detection of Malware has been posing a unique challenge. Malware analysis is the study of malicious code to prevent attacks.It is also helps with vulnerability assessment. This article aims for classification of malware using a deep learning model to obtain an accurate and efficient performance. Our system extracts a number of features and trains the Long Short-Term Memory (LSTM) model. The study utilises hyper- parameter tuning which to improve the accuracy and efficiency of the model. The findings revealed 99.65% accuracy using sigmoid function that outperforms other activation function. This can be helpful in malware detection.

Biography

Saba Iqbal is a Security Analyst at Pure Health group, Speaker at the 15th International Conference on Information Technology and Applications (ICITA 2021) conference. She earned her Master's of science in Network Security and Bachelors in Electrical & Electronics. She is the of author a peer-reviewed publication in the area of data science and network security at Springer.