Malware Classification using Back-Propagation based Artificial Neural Networks

Anurag Datta Roy
anuragdattaroy@gmail.com

Rajat Tripathi
rajat.kumar6@learner.manipal.edu

Suyash Shetty
suyash.shashikant@learner.manipal.edu

Department of Computer Science and Engineering
Manipal Institute of Technology

Introduction

A major and serious threat on the Internet today are malicious software or data which seek to damage users' systems. Malware identification and classifcation is one of the most important research problems in digital forensics. Malware binaries are set of instructions which may affect your system without your permission. Most research in this area has relied on specific API calls, sequences of bytes, statistical analysis etc. The proposed method uses digital image processing and machine learning techniques to detect and classify malware entities and is expected to perform much better than traditional techniques.

Proposed Method

Malware binaries are a set of instructions consisting of a sequence of 1s and 0s. These binaries can hence be reshaped in the form of a 2-dimensional matrix and represented as a grayscale image. By observing malware images of all available variants and their texture similarities, we have sufficient motivation to classify malware based on texture features. The gray scale images will be preprocessed and features will be extracted from them using feature engineering which will then be fed to a neural network. Using gradient descent optimization and back propagation, the neural network will learn to distinguish the features and the textures in the images.

Objective

The objective of this project is to identify a behaviour of malicious data based on global features by building a model that classifies malware with high true positive and very low false positive rates.

Expected Results

With sufficient data and training, the proposed model should achieve greater than 90% true positive accuracy and ~1% false positive rate.