2019 15th International Conference on Electronics, Computer and Computation (ICECCO)

Enhanced Decision Tree-J48 With SMOTE Machine Learning Algorithm for Effective Botnet Detection in Imbalance Dataset

by

Ilyas Adeleke Jimoh; Idris Ismaila; Morufu Olalere

Abstract

Botnet is one of the major security threats in the field of information technology today (IT). The increase in the rate of attack on industrial IT infrastructures, theft of personal data and attacks on financial information is becoming critical. Majority of available dataset for botnet detection are very old and may not be able to stand the present reality in this research area. One of the latest datasets from Canadian Institute of Cyber Security labeled “CICIDS2017” was noted as an imbalance data distribution ratio of 99% to 1%. This distribution represents majority to minority class ratio. This may pose a challenge of over-fitting in majority class to the research and create a bias in the analysis of results. This research work has adopted J48 decision tree machine learning algorithm with application of SMOTE technique in solving the problem of imbalance dataset, thereby leading to an improved detection of botnets. The accuracy of the highest scenario was 99.95%. This is a significant improvement in detection rate compare to the previous research work.

https://ieeexplore.ieee.org/document/9043262