Abstract

Distributed Denial of Service (DDoS) attacks are increasingly utilized and are causing an enormous threat to the availability and stability of network systems these days. The majority of existing anomaly detection approaches struggle to determine new or novel instances of attack. In this study, a deep autoencoder model is used to detect such threats by classifying data as normal or anomalous even without labeled data.The model is trained for reconstructing the input patterns, and large reconstruction errors are used as the identifiers of potential anomalies.Depending on the nature of the dataset, preprocessing operations such as data cleaning, normalization, and feature selection are applied to retain the most relevant features. To separate true activity from potential danger, a detection threshold is created using the ROC curve, balancing sensitivity with low rates of false positives. The model was evaluated on the CIC-DDoS 2019 dataset and had strong performance, producing precision, recall, and F1 measures of 97%. Compared to other unsupervised learning methods applied to the same set of data, it performed better in detecting new attacks, yielding stronger security and fortifying system security overall.

Indeks Terms – anomaly detection, unsupervised learning, deep autoencoder, thresholding reconstruction error.