INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

DCAE-CIDS: A Denoising Cooperative Cloud Intrusion Detection System based on Deep Learning

A Dissertation by

Mr. Nujitha Wickramasurendra

Supervised by

Mr. Saman Hettiarachchi

Submitted in partial fulfilment of the requirements for the BEng in Software Engineering degree at the University of Westminster.

May 2022

ABSTRACT

Intrusion Detection System (IDS) refers to detecting abnormal behaviours or threat patterns in a system environment in which it is adopted. It is increasingly becoming more difficult for standalone IDSs to withstand detecting these new types of malicious attacks as their knowledge level is limited to a set of known threat patterns. And it has been found that cooperative IDS mechanisms have increased the detection rate up to 60% over the traditional standalone approaches. When performing intrusion detection in a real-time setting an IDS must be more reliable in predicting traffic statuses though it receives partial or incomplete feedback from consulted IDSs.

This project focuses on addressing this limitation by applying a deep learning (DL) approach which is using Denoising Convolutional Autoencoder to the IDS and improving the robustness of detection by reconstructing such corrupted data while leveraging the cooperation among IDSs. The system is trained and tested based on the KDD’99 benchmarking dataset.

The results show that the system achieves better results where it scores 95% accuracy under corrupted data and 99% accuracy with original data in multi-class classification. The system has been evaluated using standard evaluation metrics: precision, recall, f1 score, AUC-ROC, and overall accuracy levels.

Keywords: Cyber-Security, Cloud Computing, Network Intrusion Detection System, Denoising Auto-Encoder, TensorFlow, CNN