INFORMATICS INSTITUTE OF TECHNOLOGY

IN COLLABORATION WITH

UNIVERSITY OF WESTMINSTER

Quality Assurance Software
For Network Anomaly Detection

A Project Proposal by

Mr. Inura Dewage

Supervised by

Mr. Prashan Saminda Rathnayake

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

April 2023

ABSTRACT

With the rapid growth of computers and networks, our daily work has become more efficient, thanks to the widespread use of the internet and IoT technologies. However, this progress has also led to an increase in malicious attacks targeting these systems. Among the various types of attacks, DoS attacks pose a significant threat. Unfortunately, DoS attacks have become a favorite choice for hackers, and their prevalence continues to rise.

To address this escalating problem, there is a need for lightweight network attack detection methods. Many organizations employ network management systems (NMS) to ensure the smooth operation of their networks. However, most of these organizations focus solely on network performance monitoring and overlook network security. Yet, the data collected by NMS holds tremendous potential for detecting and mitigating network anomalies.

This paper presents an effective mechanism for network anomaly detection using machine learning and SNMP MIB data. The primary motivation behind this project is to develop a lightweight attack detection mechanism that can be deployed in any network without limitations. SNMP, being a lightweight protocol integrated into almost every network, serves as an ideal choice for this purpose.

Machine learning plays a crucial role in enhancing the power of SNMP data by employing classification techniques. This project will explore various machine learning techniques and demonstrate their effectiveness in utilizing NMS data gathered using RFC-1213 MIB (Management Information Base) to detect network anomalies, particularly DoS attacks.

By leveraging the capabilities of machine learning and the rich data provided by SNMP MIB, this project aims to develop a robust and efficient network anomaly detection system. The goal is to enable organizations to proactively identify and respond to network attacks, ultimately ensuring the security and reliability of their networks.