ABSTRACT

The increasing reliance on internet connectivity has heightened cybersecurity risks, particularly at the end-user level. This research proposes a comparative evaluation of two Intrusion Prevention Systems (IPS): a traditional Snort-based IPS and a machine learning-based IPS. While Snort relies on predefined rule sets to detect threats, it often fails to identify novel or evolving attack patterns. In contrast, the machine learning approach utilizes a Decision Tree classifier trained on network flow data to detect anomalies based on statistical features.

The experimental setup involves a Linux-based cloud server subjected to simulated network attacks, including Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS), originating from Docker-based attacker containers. Traffic is captured, processed, and classified to assess each system's effectiveness in detecting and blocking malicious flows. Performance metrics such as accuracy, precision, recall, and false positive rate are used for evaluation.

Results demonstrate that the machine learning-based IPS outperforms the Snort system in detecting attacker flows while producing fewer false positives for benign client traffic. This research highlights the advantages of data-driven intrusion prevention and its applicability in modern, lightweight network environments.

Keywords: Network Security, Intrusion Prevention System, Snort, Machine Learning, Decision Tree.