ABSTRACT

The extensive proliferation of IoT devices has led to a massive increase in IoT-based DDoS attacks, which is posing a critical threat to smart home networks and other IoT-connected ecosystems. Existing security solutions lack the ability to identify new and sophisticated IoT malware variants effectively. This paper presents a machine learning-based approach using the K-Nearest Neighbor (KNN) classifier and its Bagging ensemble variant to identify diverse DDoS attacks like SYN Flood, UDP Flood, and Mirai botnet variants in IoT network traffic. In this work, the CICIoT2023 dataset and correlation-based feature selection method are utilized to identify the most impactful attributes to categorize attacks. Experiments demonstrate that the baseline KNN model achieves outstanding accuracy, precision, recall, and F1-score greater than 97% with less computational overhead compared to the ensemble approach, thus being deployable in real-time in low-resource IoT environments. This article demonstrates the feasibility of lightweight machine learning models to realize effective and efficient intrusion detection in smart home IoT networks. Subsequent research will explore more complex feature engineering and ensemble learning frameworks for enhanced detection of novel attack behaviors.

Keyword : Distributed Denial of Service, IoT Botnets, Machine Learning, K-Nearest Neighbor, Smart Home Security