abtechchennai@gmail.com
www.abtechnologies.in
9840511458

IOT-KEEPER: DETECTING MALICIOUS IOT NETWORK ACTIVITY USING ONLINE TRAFFIC ANALYSIS AT THE EDGE

ABSTRACT

IoT devices are notoriously vulnerable even to trivial attacks and can be easily compromised. In addition, resource constraints and heterogeneity of IoT devices make it impractical to secure IoT installations using traditional endpoint and network security solutions. To address this problem, we present IOTKEEPER, a lightweight system which secures the communication of IoT. IOT-KEEPER uses our proposed anomaly detection technique to perform traffic analysis at edge gateways. It uses a combination of fuzzy C-means clustering and fuzzy interpolation scheme to analyze network traffic and detect malicious network activity. Once malicious activity is detected, IOT-KEEPER automatically enforces network access restrictions against IoT device generating this activity, and prevents it from attacking other devices or services. We have evaluated IOT-KEEPER using a comprehensive dataset, collected from a real-world test bed, containing popular IoT devices. Using this dataset, our proposed technique achieved high accuracy (≈0:98) and low false positive rate (≈ 0:02) for detecting malicious network activity. Our evaluation also shows that IOT-KEEPER has low resource footprint, and it can detect and mitigate various network attacks without requiring explicit attack signatures or sophisticated hardware.