

## Botnet Detection with ML Techniques by Using the BoT-IoT Dataset

**Authors :** Adnan Baig, Ishteeaq Naeem, Saad Mansoor

**Abstract :** The Internet of Things (IoT) gadgets have advanced quickly in recent years, and their use is steadily rising daily. However, cyber-attackers can target these gadgets due to their distributed nature. Additionally, many IoT devices have significant security flaws in their implementation and design, making them vulnerable to security threats. Hence, these threats can cause important data security and privacy loss from a single attack on network devices or systems. Botnets are a significant security risk that can harm the IoT network; hence, sophisticated techniques are required to mitigate the risk. This work uses a machine learning-based method to identify IoT orchestrated by botnets. The proposed technique identifies the net attack by distinguishing between legitimate and malicious traffic. This article proposes a hyperparameter tuning model to improve the method to improve the accuracy of existing processes. The results demonstrated an improved and more accurate indication of botnet-based cyber-attacks.

**Keywords :** Internet of Things, Botnet, BoT-IoT dataset, ML techniques

**Conference Title :** ICCEEE 2025 : International Conference on Computing, Electrical and Electronic Engineering

**Conference Location :** Amsterdam, Netherlands

**Conference Dates :** January 23-24, 2025