IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Smart-shield: Dual Phase ML Defense for IoT BotNet Threats

Abhinav Murkute, Tejas Fulzele, Yash Lase, Kundan Kumar, Prof. D.G. Jadhav
Department of Information Technology
Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: *Botnet attacks are one of the most prevalent and harmful threats in the Internet of Things (IoT) ecosystem. These attacks typically begin with a reconnaissance or scanning phase and eventually lead to large-scale Distributed Denial of Service (DDoS) assaults. Current detection methods often focus on identifying botnet activity only after IoT devices have already been compromised and are actively participating in DDoS attacks. Additionally, many of these techniques are restricted to specific datasets, which limits their effectiveness across different environments due to variations in attack behaviors. To overcome these limitations, this study introduces a diverse and comprehensive dataset that includes 33 types of scanning attacks and 60 types of DDoS attacks. The dataset is constructed using samples from three widely recognized public datasets, enhancing the model's ability to generalize across various attack patterns. The paper presents a novel Dual Phase Machine Learning Defense strategy for countering IoT botnet threats. In the first phase, a ResNet-18 model is trained to detect scanning behaviors at the early stage of an attack, enabling timely prevention. In the second phase, another ResNet-18 model is utilized to identify DDoS attacks, ensuring effective detection of botnet activities. The proposed method delivers high performance with an accuracy of 98.89%, precision of 99.01%, recall of 98.74%, and an F1 score of 98.87%, showcasing its effectiveness in both detecting and preventing IoT botnet threats.*

Keywords: IoT Botnet Attacks, ResNet-18, DDoS Detection, Scanning Attack Prevention, Two-Phase Machine Learning, Intrusion Detection System (IDS)

DOI: 10.48175/568