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 1, May 2025

Impact Factor: 7.67

Enhanced Botnet Attack Detection in IoT Environment

B. Swetha[1], K. Srirag Reddy[2], J. Santhosh[3]

Assistant Professor, Department of IT[1]

B.Tech Student, Department of IT[2,3]

Mahatma Gandhi Institute of Technology, Hyderabad, India

Abstract: *This study introduces a detailed framework for detecting botnets that utilizes cutting-edge machine learning techniques to boost both accuracy and reliability. The framework combines bagging methods like Random Forest and Bagged Decision Trees with boosting algorithms such as XGBoost and LightGBM to achieve outstanding model generalization. To fine-tune feature selection, it employs Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA), ensuring that the most pertinent features from network traffic data are extracted. The system tackles data quality issues through thorough cleaning, normalization, and correcting class imbalances using the Synthetic Minority Over-sampling Technique (SMOTE). When tested on the UNSW-NB15 dataset, this proposed framework shows remarkable performance, achieving high accuracy and a strong precision-recall area. The results underscore its effectiveness in identifying botnet attacks and its promise as a scalable solution for bolstering network security*

Keywords: network security

DOI: 10.48175/568