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 6, Issue 3, January 2026

Impact Factor: 7.67

Deep Learning-Based Intrusion Detection System for High-Speed Networks

Kiran Yadav[1] and Anuradha Pathak[2]
Research Scholar, Dept of Electronics & Communication[1]
Asst. Prof., Dept of Electronics & Communication[2]
NITM, Gwalior India
kiran085@gmail.com, anuradha.pathak27@gmail.com

Abstract: *The rise in IoT devices and their diverse applications has heightened the importance of IoT security. Research on network security indicates that Distributed Denial of Service (DDoS) attacks on IoT systems are becoming more frequent, advanced, and varied. DDoS attacks have evolved into serious cyber threats, enabling lucrative and efficient cybercrimes. Among the most hazardous risks to network security, DDoS attacks present significant challenges for machine learning (ML)-based detection systems, often impacting their accuracy. Artificial intelligence (AI), which integrates ML for cyberattack detection, is the most widely used approach in this domain. This study proposes a model for identifying and reducing DDoS attacks in Software-Defined Networking (SDN) using ML techniques. The model compares the F1-score, recall, accuracy, and precision of various ML algorithms, incorporating Extra Tree and Cat Boost classifiers. To enhance detection capabilities, DDoS-Net effectively addresses data imbalance and incorporates a comprehensive feature analysis.The evaluation of DDoS-Net on the UNSW-NB15 dataset highlights its outstanding performance. The most significant level of accuracy attained using Cat Boost and Extra Tree classifiers is 90.78%, 90.27%, respectively. This research introduces a robust and accurate method for detecting DDoS attacks, significantly enhancing cyber security measures and reinforcing digital infrastructures against these persistent threats.*

Keywords: IoT Security, DDoS Attacks, Cyber Threats, Machine Learning , Network Security

DOI: 10.48175/IJARSCT-30903