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, November 2025
Impact Factor: 7.67

Intrusion Detection System Using AI and Deep Learning

Sowndarya C R and Suchi Raj R
Department of MCA
Vidya Vikas Institute of Engineering and Technology, Mysuru, India
sowndaryacrgowda@gmail.com, suchi.raj2010@gmail.com

Abstract: *In today's digital landscape, cybersecurity is a paramount concern, with network intrusion detection systems (IDS) playing a vital part in protecting infrastructure and data. The undertaking Using state-of-the-art machine learning methods, namely Recurrent Neural Networks (RNNs) with Long Short-Term Memory (LSTM) units, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" overcomes the shortcomings of conventional IDS. This study leverages the NSL-KDD dataset to train a robust IDS capable of identifying various types of network attacks including Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probing attacks. Our approach concentrates on identifying the temporal trends in network traffic data, which are essential for differentiating between benign and malevolent activity. When In contrast to traditional machine learning techniques, the RNN-LSTM model showed greater accuracy and precision, greatly lowering both false negatives and false positives. This study describes the RNN-based IDS's design, implementation, and evaluation, highlighting its potential. to improve cybersecurity measures in contemporary networks. The results highlight The importance of sophisticated machine learning approaches in developing effective and adaptive security solutions capable of addressing the evolving threat landscape..*

Keywords: recurrent neural networks, deep learning, machine learning, prediction,dos, r2l,u2r.attack

DOI: 10.48175/IJARSCT-29966