Enhanced Cybersecurity for Network Intrusion Detection System Based Artificial Intelligence (AI) Techniques

Mani Gopalsamy
Senior Cyber Security Specialist, Louisville, KY, USA
manigopalsamy14@gmail.com

Abstract*: Cybersecurity has risen to the pinnacle of technological concern due to the exponential growth in the variety and sophistication of cyberthreats. Network attacks are currently the most urgent problem facing contemporary civilization. To identify and stop hostile assaults inside networks, there has to be an intrusion detection system in place. In several industries, most notably information security, effective detection systems for intrusions are being developed using machine learning and deep learning. This is an investigation of how ML methods may be used to enhance cybersecurity defences, with a focus on network intrusion detection, prevention, and response. This study inspects the efficacy of machine learning, utilising CNN, ANN, and LSTM, and assesses them using F1-score, accuracy, recall, and precision. Outcomes demonstrate that CNN outperforms other models, achieving 99% in all key metrics, making them highly effective for detecting network intrusion. However, the study's reliance on the NSL-KDD dataset presents limitations, as it may not fully capture modern network intrusion. Future research should incorporate more recent datasets, real-time performance evaluations, and hybrid models to improve network intrusion detection accuracy and efficiency.*

Keywords: Cybersecurity, network intrusion classification, detection, NSL-KDD dataset, machine learning, CNN