**Network Intrusion Detection System Using Deep Learning**

**Abstract:**

In the current digital environment, network security has become an urgent issue due to the increasing frequency of advanced cyberattacks. This project introduces a Network Intrusion Detection System (NIDS) that utilizes deep learning methods to effectively detect malicious behaviors in network traffic. A hybrid model combining CNN and LSTM is developed to leverage both spatial and temporal characteristics of the data, improving detection performance. The model is trained and assessed using the UNSW-NB15 dataset, which includes a variety of modern attack types alongside regular traffic. The system achieves an impressive 98% accuracy in binary classification (normal versus attack) and 83% accuracy in multi-class classification (recognizing specific attack types). These outcomes emphasize the promise of integrating Convolutional Neural Networks and Long Short-Term Memory networks to create a robust and intelligent framework for intrusion detection in contemporary network environments.

**Keywords**: Deep Learning, Intrusion Detection, CNN-LSTM, Cybersecurity, Network Attacks