- Application Area: Intrusion Detection Systems (IDS)

Topic:

Anomaly-Based Intrusion Detection in Network Traffic

- Problem Statement:

Traditional signature-based intrusion detection systems (IDS) are limited to detecting known attack patterns and often fail to identify new or sophisticated attacks. As cyber threats evolve, there is a critical need for systems that can detect anomalies in network traffic indicative of potential intrusions or breaches. The challenge is to develop a machine learning model that can automatically detect abnormal network behavior that could signify an intrusion, even if the specific attack signature is unknown.

- Solution:

A machine learning model will be developed to analyze network traffic data and detect deviations from typical patterns that could indicate a security breach. The model will be trained on a dataset containing both normal and abnormal network traffic, learning to differentiate between benign activities and potential threats. The model's ability to generalize will allow it to detect previously unseen attack patterns.

- Dataset:

The dataset used for this project is the NSL-KDD Dataset, which is a refined version of the KDD'99 dataset and is publicly available. It contains a large number of network traffic records labeled as either normal or malicious (e.g., DoS attacks, R2L, U2R, and probing attacks). The dataset is accessible from the NSL-KDD repository.

- Machine Learning Algorithm:

The Support Vector Machine (SVM) algorithm will be used for classification. SVM is effective for high-dimensional spaces and can be tailored to detect anomalies by identifying the boundary between normal and abnormal data points. Additionally, Autoencoders— a type of neural network— can be used for unsupervised anomaly detection by learning a compressed representation of the data and flagging anomalies as outliers.