***Network Anomaly Detection:***

**Abstract:**

Network security is crucial in the highly connected digital world of today. The traditional rule-based intrusion detection systems (IDS) frequently struggle to detect complex attacks. Techniques based on machine learning have showed promise in advancing network anomaly detection using artificial intelligence (AI) techniques. In order to analyse network traffic patterns and spot anomalous activity suggestive of potential security concerns, this project intends to construct an AI-based Network Anomaly Detection system. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs), among other deep learning models, are used by the system to detect anomalies in real time. We can Incorporating supervised learning techniques into a network anomaly detection project can significantly enhance the system's ability to distinguish between normal and anomalous network behaviour, leading to more accurate and efficient threat detection and response. The project's main goals are to improve network security systems' precision, effectiveness, and agility while avoiding false positives and assuring quick reaction to emerging threats.

**Problem Statement:**

Network security is crucial in the connected and data-dependent world of today. Organizations must contend with a constantly evolving threat landscape of sophisticated cyberattacks that have the potential to interfere with business operations, jeopardize data integrity, and invade the privacy of critical data. Traditional rule-based network security solutions are frequently not enough to adequately detect and address evolving threats. To address this challenge, there is a need for an AI-based network anomaly detection system that can proactively identify and mitigate network anomalies, intrusions, and suspicious activities.