AI-Powered Intrusion Detection System

Abstract: -

Intrusion Detection Systems (IDS) play a pivotal role in safeguarding computer networks within the cybersecurity domain, serving as a critical defense mechanism against threats and vulnerabilities. To create highly so effective IDS solutions, the utilization of various machine learning methods has become commonplace. Among these methods, ensemble learning has consistently demonstrated its efficacy in learning and adapting to emerging threats. In this paper, we would like to introduce an innovative Intrusion Detection System that harnesses the power of ensemble machine learning techniques.

In our pursuit of improving classification accuracy and reducing false positives, we selected pertinent features from the comprehensive CICIDS dataset. These carefully curated features form the foundation of our intrusion detection model. Our approach incorporates a trifecta of machine learning algorithms, including decision trees, random forests, and Support Vector Machines (SVM), to construct a robust IDS.

In an era of escalating cyber threats, the need for robust and adaptive Intrusion Detection Systems (IDS) has never been more critical. Traditional rule-based and signature-based IDS solutions have limitations in detecting sophisticated and evolving threats. This project introduces an innovative AI-Powered Intrusion Detection System that leverages cutting-edge machine learning and deep learning techniques to enhance network security.

Our IDS is designed to autonomously analyse vast amounts of network traffic data in real-time, detecting anomalies and potential security breaches. It utilizes advanced machine learning algorithms, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to learn intricate patterns in network behaviour. This adaptability enables the system to identify novel and previously unseen attack vectors, offering a proactive defense mechanism.