VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY
Permanently Affiliated to JNTU Kakinada, Approved by AICTE
Accredited by NAAC with 'A' Grade, ISO 9001:2008 Certified
Nambur, Pedakakani (M), Guntur (Dt) - 522508
Department of CSE - Artificial Intelligence & Machine Learning

TL: A. Tejaswini(21BQ1A4204) TM1:K.DurgaDevi(21BQ1A4256) TM2: A.Bhargav(21BQ1A4264) TM3: Bharath (21BQ5A4204)	**Batch : CSM-A:: 10**	Guide Name : B.Pardha Saradhi

Project Title : Intrusion Detection System

Abstract

An Intrusion Detection System (IDS) using machine learning is a security mechanism designed to monitor network traffic or system activities for malicious actions or policy violations. Traditional IDS tools rely on signature-based or rule-based detection, which can struggle to identify new or evolving threats. Machine learning-based IDS improves on this by leveraging algorithms that can learn patterns in data, detect anomalies, and even predict potential attacks in real time. These systems are particularly useful in environments with high data volumes, where manual monitoring or static rules would fail to scale effectively.

The core of the project involves collecting and preprocessing data to train machine learning models. The data typically comes from network traffic logs or system logs and includes both normal and malicious activity. This dataset is labeled to help the model learn what constitutes normal versus malicious behavior. Features such as IP addresses, packet sizes, and protocol types are extracted to provide inputs for the machine learning algorithm. Once preprocessed, the data is split into training and testing sets for building and evaluating the model.

Several machine learning techniques can be applied to IDS, including supervised learning (e.g., decision trees, support vector machines, and neural networks) and unsupervised learning (e.g., clustering algorithms). Supervised models require labeled data, which makes them highly effective but dependent on the quality and quantity of labeled examples. Unsupervised models, on the other hand, detect anomalies by identifying patterns that deviate from the norm, making them suitable for discovering previously unknown threats. Ensemble methods, which combine multiple algorithms, are also common to improve detection accuracy.

The evaluation of the IDS is a critical step in the project. Metrics such as accuracy, precision, recall, and the F1 score are used to measure the system's performance in identifying intrusions without generating excessive false positives. The system is often tested on benchmark datasets like KDD CUP 99, NSL-KDD, or CICIDS2017 to validate its robustness. Real-time implementation may involve deploying the model in a live network environment and continuously refining it using online learning techniques to adapt to new threats.

Signature of
Guide

Signature of
Project Co-ordinator