**Project Title:** Intrusion Detection System for DDoS Attacks

**Problem Statement:**

* Analysis and detection Dos/DDoS attacks on a real time server.
* Deployment of AI-enabled model over a server.

**Objective:**

* To design a model to prevent DDoS Attack on any cloud based server.
* To deploy a model over a cloud server which can analyse and detect any attack on real time.

**Proposed Solution:** The methodology for this project involves several key steps:

1. **Literature Review:**
   * Conduct a comprehensive review of existing Intrusion Detection System (IDS) techniques and DDoS attack patterns. This will include studying various machine learning and deep learning approaches that have been previously used to detect such attacks.
2. **Data Collection:**
   * Gather extensive datasets containing both normal and attack traffic. These datasets will be used for training and testing the IDS. The data collection process will ensure a diverse range of attack types and patterns to enhance the model’s detection capabilities.
3. **Feature Selection:**
   * Identify and select key features that can effectively distinguish between normal and malicious traffic. This step is crucial for improving the accuracy and efficiency of the IDS.
4. **Model Development:**
   * Develop a machine learning-based IDS using advanced techniques such as neural networks, support vector machines, or ensemble methods. The model will be trained to recognize and respond to DDoS attack patterns.
5. **Evaluation:**
   * Test the IDS on benchmark datasets to measure its performance. Key metrics for evaluation will include accuracy, precision, response time, scalability, resource utilization, and robustness. This step will ensure that the model meets the required standards for real-world deployment.
6. **Mitigation Strategies:**
   * Implement and test various strategies to mitigate the impact of detected DDoS attacks. This may include rate limiting, traffic filtering, and other defensive measures to ensure the server remains operational during an attack.

**A diagram of data collection

Description automatically generated**

**Expected Outcome:**

1. A robust IDS capable of detecting DDoS attacks with high accuracy, ensuring the security and stability of cloud-based servers.
2. A comprehensive evaluation of the IDS performance on real-world datasets, demonstrating its effectiveness and reliability.
3. Effective mitigation strategies that can be deployed alongside the IDS to reduce the impact of DDoS attacks, ensuring minimal disruption to services.