**DDOS ATTACK DETECTION & MITIGATION**

**ABSTRACT:**  
This project focuses on detecting and mitigating Distributed Denial of Service (DDoS) attacks in IoT environments using machine learning and deep learning algorithms. Due to the limited processing power and battery capacity of IoT devices, traditional antivirus solutions are impractical. Instead, lightweight ML/DL approaches such as XGBoost and CNN are employed to achieve high detection accuracy—over 95%—using the IoT23 DDoS attack dataset. The system processes and trains models in Jupyter Notebook and deploys a Flask web application for real-time attack detection. Upon identifying an attack, the system automatically blocks the attacker’s IP address via firewall rules, preventing future malicious access. Evaluation metrics such as accuracy, precision, recall, confusion matrix, and F-score demonstrate the effectiveness of the proposed approach in securing IoT networks from DDoS threats.

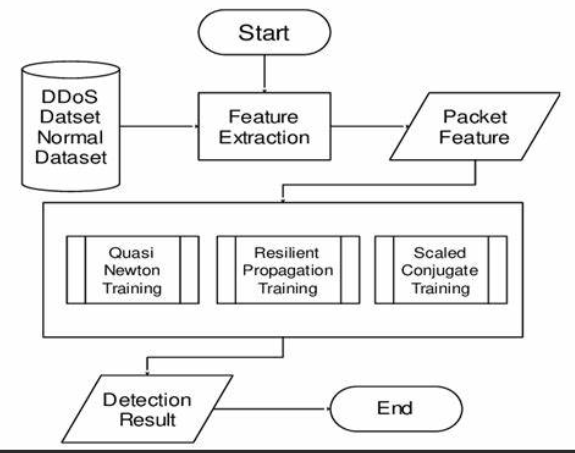
Bottom of Form

### EXISTING SYSTEM

In existing IoT security solutions, traditional antivirus software is generally used to detect and prevent network attacks. However, these antivirus programs are resource-intensive and unsuitable for IoT devices due to their limited processing power and battery life. Some systems employ rule-based detection methods which are computationally light but suffer from low accuracy and high false positives. Machine learning models like simple classifiers have also been applied, but their detection capabilities are limited when handling complex or evolving DDoS attacks in IoT networks. Overall, existing systems either lack efficiency or accuracy in detecting DDoS attacks in resource-constrained IoT environments.

### PROPOSED SYSTEM

The proposed system leverages advanced machine learning and deep learning algorithms—specifically XGBoost and CNN—to detect DDoS attacks in IoT networks with high accuracy and efficiency. Using the IoT23 DDoS attack dataset, the models are trained to distinguish between normal and malicious network traffic, achieving detection accuracies above 95%. The system integrates a real-time detection mechanism through a Flask web framework, which monitors incoming IoT network requests. Upon detecting an attack, the system automatically updates firewall rules to block the source IP address, thereby mitigating the attack and protecting the IoT devices from further harm. This approach offers a lightweight, scalable, and accurate solution tailored for the resource-constrained nature of IoT environments.



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* Hard Disk  :   40 GB.
* Ram    :   512 MB.

**SOFTWARE REQUIREMENTS:**

* Operating system   : Windows 7
* Coding Language  : python