# ABSTRACT

## AI Web Application Firewall

An **AI-powered Web Application Firewall (AI-WAF)** is an advanced security solution designed to protect web applications by **analyzing and preventing malicious traffic in real-time**. It leverages **artificial intelligence and machine learning** to detect complex cyber threats, surpassing the capabilities of traditional rule-based WAFs. The AI-WAF **inspects all incoming HTTP/HTTPS requests**, including headers, payloads, cookies, URLs, and encrypted traffic, to identify potential threats such as **SQL injection, cross-site scripting (XSS), and DDoS attacks**. By utilizing **supervised and unsupervised machine learning models** along with **Natural Language Processing (NLP)**, it dynamically classifies traffic and adapts to evolving attack patterns. One of its key features is **adaptive learning**, which enables continuous evolution by analyzing traffic data and integrating **real-time threat intelligence feeds** to block traffic from malicious IPs and domains. Administrators benefit from **custom rule management**, allowing them to define specific blocking rules, whitelist trusted IPs, and tailor security policies to meet their application's unique needs, reducing **false positives** and enhancing accuracy. The AI-WAF also includes **rate-limiting capabilities** to prevent abusive traffic or brute force attacks by throttling requests based on frequency. Another critical functionality is **risk scoring**, where each incoming request is evaluated and assigned a risk score based on factors such as **IP reputation, payload behavior, and request frequency**, ensuring high-risk requests are flagged or blocked while legitimate traffic flows seamlessly. To mitigate automated threats, the AI-WAF implements **bot mitigation techniques**, identifying malicious bots through **behavioral analysis** like mouse movements and typing patterns, and adds **CAPTCHA challenges** for additional security. It also offers robust **DDoS protection** by detecting unusual traffic spikes and blocking repetitive patterns. A **centralized dashboard and monitoring system** provide administrators with **real-time analytics, traffic trends, and detailed logs** to ensure compliance with regulations such as **GDPR and HIPAA**. Deployment is highly flexible, allowing the AI-WAF to be integrated into **on-premises or cloud environments** using tools like **Docker and Kubernetes** for scalable microservices and high availability. By combining **intelligent traffic analysis, real-time threat detection, adaptive learning, and comprehensive monitoring**, an AI-WAF ensures modern web applications are protected from evolving cyber threats, offering a scalable, efficient, and indispensable layer of security.

## EXISTING SYSTEM: -

- **Purpose**: Protects websites from attacks.
- **Method**: Uses fixed rules to block attacks.
- **Attack Detection**: Blocks known attacks.
- **Adaptability**: Less flexible.
- **False Positives**: More mistakes blocking safe actions.
- **Protection**: Good against known threats.
- **Maintenance**: Needs regular updates.
- **Learning**: Does not learn from traffic.
- **Overall Security**: Solid protection.

## PROPOSED SYSTEM: -

- **Purpose:** Protects websites using AI.
- **Method:** Learns and adapts to new attacks.
- **Attack Detection:** Detects new and unknown attacks.
- **Adaptability:** More flexible and adaptive.
- **False Positives:** Fewer mistakes, understands context.
- **Protection:** Better against new and unknown threats.
- **Maintenance:** Updates itself continuously.
- **Learning:** Learns from traffic patterns.
- **Overall Security:** Advanced and adaptive protection.