National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

A Study of SMART MITIGAT's Functionality on The Service Firewall Architecture

Moram Sunil Kumar Reddy

Research Scholar, Ph.D. in Computer Science and Engineering,
Dr. A.P.J. Abdul Kalam University, Indore, M.P., India.

ABSTRACT

The increasing complexity of cyber threats necessitates advanced security mechanisms to protect digital infrastructures. SMART MITIGAT, an intelligent security framework, enhances the functionality of service firewall architectures by integrating adaptive threat detection and real-time mitigation strategies. This paper explores how SMART MITIGAT leverages artificial intelligence (AI), machine learning (ML), and behavioral analytics to strengthen firewall defenses against evolving cyberattacks. Traditional firewalls often struggle with dynamic threats, but SMART MITIGAT introduces automated anomaly detection, deep packet inspection, and predictive threat modeling to proactively neutralize potential risks. By employing a self-learning mechanism, the system continuously refines its defense strategies, ensuring minimal false positives while effectively blocking malicious traffic. Additionally, its integration with software-defined networking (SDN) and cloud-based security solutions enhances scalability and flexibility, optimizing network performance without compromising protection. The study also examines SMART MITIGAT's role in mitigating Distributed Denial of Service (DDoS) attacks, ransomware, and zero-day exploits by enforcing real-time access control policies and dynamic rule adjustments. Findings suggest that implementing SMART MITIGAT within service firewall architecture significantly enhances security resilience, reducing the attack surface and improving overall threat response capabilities. This research highlights the necessity of intelligent, automated security frameworks to counteract modern cyber threats efficiently.