SmartGuard: A Machine Learning Based Classification Framework for Automated DoS/DDoS Defence in Next Generation Firewall Systems

Domain: Cybersecurity and ML Applications

Abstract:

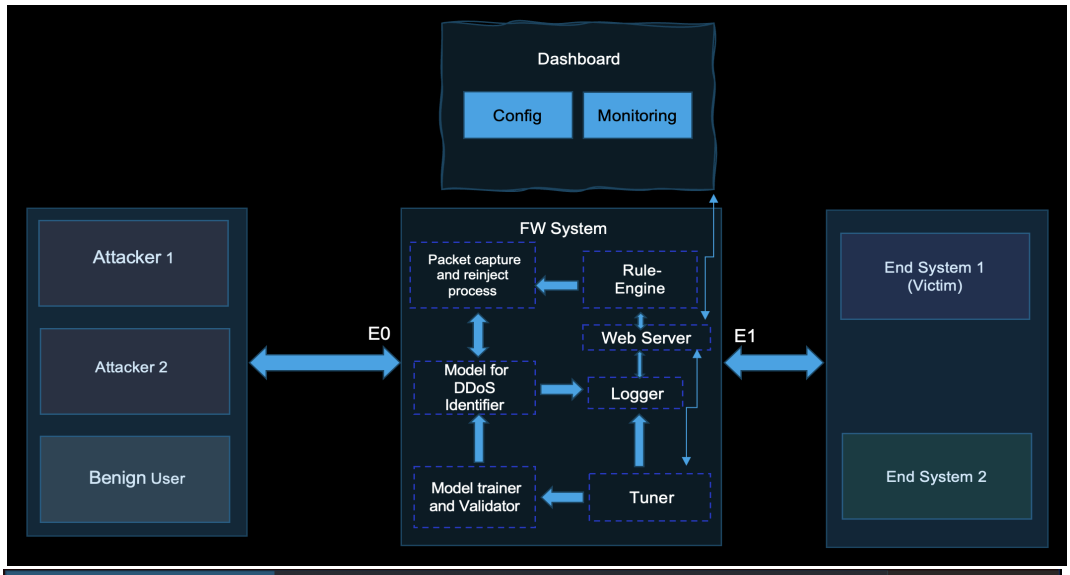
Today's cyber threat landscape is rapidly evolving, with attackers using sophisticated and AI-driven techniques to exploit vulnerabilities. Modern threats include Distributed Denial of Service (DDoS) attacks and fast-spreading malware capable of stealing data, causing financial loss, and compromising critical systems.

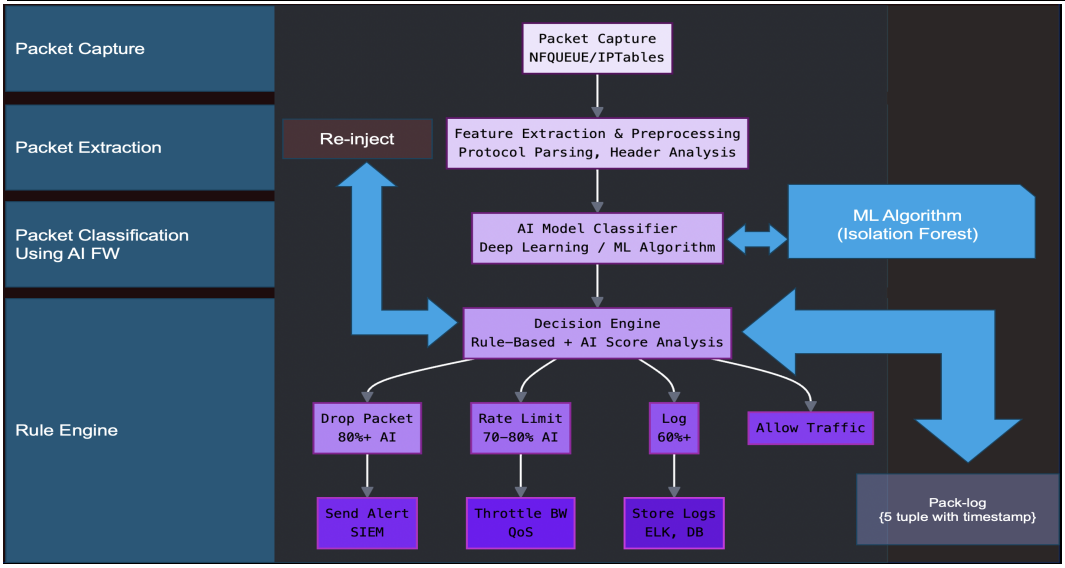
For example, in a BYOD (Bring Your Own Device) environment, an employee's system may get infected while using an unsecured network. Once connected to the corporate network, the malware could begin port scanning and spreading across internal systems, eventually forming a botnet capable of launching a coordinated DDoS attack. With AI-powered malicious software adapting to detection methods, traditional security solutions are no longer sufficient.

To counter these threats, an AI-based detection and prevention engine is developed and trained on large datasets of known DoS/DDoS attack patterns. Integrated into existing firewall infrastructures, it continuously monitors network traffic, classifies malicious behaviour in real time, and automatically enforces security policies. Unlike conventional methods, AI systems learn from new attack patterns, adjust to emerging threats, and detect subtle anomalies that manual monitoring may miss.

Insights are drawn from leading cybersecurity research, including work by Cisco and Palo Alto Networks, to support the goal of building SmartGuard—an AI-driven, real-time threat mitigation framework bridging the gap between legacy firewalls and modern adaptive cyber defence.

Architecture / Flow Diagram:





Supervisor:

Kundhavai K R
Assistant Professor

Team No.: 152

Pullagura Santosha	**Nitin Pandita**	**Aman Kakwani**	**Santhosh A**
PES2UG22CS418	PES2UG22CS373	PES2UG22CS055	PES2UG23CS820

Publication:

Pullagura Santosha, Nitin Pandita, Aman Kakwani, and Santhosh A.
"SmartGuard: A Machine Learning Based Classification Framework for Automated DoS/DDoS Defence in Next Generation Firewall Systems", **Paper Drafted**, 2025