

<div>SmartGuard: A Machine Learning Based Classification Framework for Automated DoS/DDoS Defence in Next Generation Firewall Systems</div>				
Domain: Cybersecurity and ML Applications				
<div><div>Abstract:</div><p>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.</p><p>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.</p><p>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.</p><p>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.</p></div>				
<div><div>Architecture / Flow Diagram:</div><div><div><div><div><div>Dashboard</div><div>ConfigMonitoring</div></div><div><div>Attacker 1</div><div>Attacker 2</div><div>Benign User</div></div><div><div>FW System</div><div><div>Packet capture and reinject process</div><div>Rule-Engine</div><div>Model for DDoS Identifier</div><div>Model trainer and Validator</div><div>Web Server</div><div>Logger</div><div>Tuner</div></div><div><div>End System 1 (Victim)</div><div>End System 2</div></div></div><div><div>E0</div><div>E1</div></div></div><div><div><div>Packet Capture</div><div>Packet Extraction</div><div>Packet Classification Using AI FW</div><div>Rule Engine</div></div><div><div>Packet Capture NFQUEUE/IPTables</div><div>Feature Extraction &amp; Preprocessing Protocol Parsing, Header Analysis</div><div>AI Model Classifier Deep Learning / ML Algorithm</div><div>Decision Engine Rule-Based + AI Score Analysis</div><div>Drop Packet 80%+ AI</div><div>Rate Limit 70–80% AI</div><div>Log 60%+</div><div>Allow Traffic</div><div>Re-inject</div><div>Send Alert SIEM</div><div>Throttle BW QoS</div><div>Store Logs ELK, DB</div><div>ML Algorithm (Isolation Forest)</div><div>Pack-log {5 tuple with timestamp}</div></div></div></div></div></div>				
Supervisor:	Team No.: 152			
Kundhavai K R Assistant Professor	Pullagura Santosha PES2UG22CS418	Nitin Pandita PES2UG22CS373	Aman Kakwani PES2UG22CS055	Santhosh A PES2UG23CS820
<div><div>Publication:</div><p>Pullagura Santosha, Nitin Pandita, Aman Kakwani, and Santhosh A.</p><p>“SmartGuard: A Machine Learning Based Classification Framework for Automated DoS/DDoS Defence in Next Generation Firewall Systems”, <b>Paper Drafted</b>, 2025</p></div>				