

# AI-Driven Adaptive Cyber Defense using Continual Learning

With the exponential growth of cyberattacks in both frequency and complexity, traditional static security solutions have become increasingly ineffective. Conventional defense systems often rely on predefined rules or periodically retrained models that fail to adapt quickly to new or evolving attack patterns. To address these challenges, this research proposes an **AI-Driven Adaptive Cyber Defense Framework using Continual Learning** that enables real-time adaptation to dynamic threat landscapes. The proposed framework integrates **continual learning**, **deep reinforcement learning**, and **adaptive anomaly detection** to continuously evolve its defense mechanisms based on new data and attack behaviors. Continual learning allows the system to acquire new knowledge from incoming threats while retaining prior information, overcoming the issue of catastrophic forgetting common in traditional AI models. Reinforcement learning agents will be employed to optimize defense policies dynamically, learning to predict, prevent, and respond to cyber incidents with minimal human intervention. Furthermore, the framework will incorporate **behavioral analytics** and **threat intelligence fusion** to enhance situational awareness and proactive defense capabilities. Experimental evaluation will be conducted using real-world datasets such as NSL-KDD, CICIDS2017, and malware repositories to assess the system's performance in intrusion detection, phishing prevention, and ransomware mitigation. The expected outcome of this research is a **self-improving, autonomous cybersecurity architecture** capable of continuous adaptation and intelligent response, ensuring long-term resilience against evolving cyber threats. This study aims to bridge the gap between static defense systems and truly intelligent, adaptive cybersecurity models. **Keywords:** Cybersecurity, Adaptive Defense, Continual Learning, Reinforcement Learning, Anomaly Detection, Intrusion Detection Systems, Artificial Intelligence.