PhD RESEARCH PROPOSAL

Title: AI-Driven Adaptive Cyber Defense Framework for Real-Time Threat Prediction and Autonomous Response

1. Introduction
Cyber attacks have evolved in complexity, exploiting vulnerabilities across cloud, IoT, and distributed systems. Traditional signature-based systems fail to detect unknown or zero-day threats. Artificial Intelligence (AI) offers significant potential to enhance real-time detection and autonomous response. This proposal aims to develop an adaptive cyber-defense model that intelligently predicts and mitigates attacks using AI-driven techniques.

2. Problem Statement
Existing cyber defense systems face limitations such as static detection models, high false positives, and delayed manual mitigation. They lack the intelligence to learn, adapt, and autonomously respond to evolving cyber threats. A unified AI-based architecture is needed to address prediction, detection, and automated defense in real-time.

3. Aim and Objectives
Aim: To develop an AI-powered adaptive cyber defense framework capable of real-time threat prediction, detection, and autonomous response.

Objectives:
• Build a hybrid AI model combining deep learning and graph neural networks for robust detection.
• Integrate reinforcement learning for autonomous mitigation decisions.
• Design an explainable AI layer for transparency and trust.
• Validate performance across benchmark datasets and real-time network traffic.

4. Research Methodology
Phase 1: Data Processing – Use CICIDS2017, NSL-KDD, UNSW-NB15 and simulated network traffic.
Phase 2: AI Threat Detection – Implement deep autoencoders, LSTM/Transformer models, and GNN for anomaly and threat detection.
Phase 3: Autonomous Response – Apply reinforcement learning (DQN/PPO) for real-time mitigation actions.
Phase 4: Explainable AI – Integrate SHAP or LIME to provide actionable explanations.
Phase 5: Validation – Evaluate using accuracy, F1-score, false positives, latency, and compare with Snort/Suricata.

5. Expected Outcomes
• A novel adaptive cyber defense framework.
• Enhanced zero-day detection accuracy and reduced response time.
• Autonomous mitigation decision engine.
• Scalable deployment for cloud, IoT, and enterprise systems.

6. Significance
This research contributes to AI and cybersecurity by introducing a unified prediction–detection–response architecture. It supports national cyber resilience and can be adopted across critical sectors such as finance, healthcare, and education.

7. Timeline (3 Years)
• Year 1 – Literature review, datasets, baseline models
• Year 2 – Hybrid AI model and RL-based response engine development
• Year 3 – XAI integration, evaluation, deployment, thesis writing

References
(1) Shone et al., Deep Learning IDS, IEEE TIFS.

(2) Moustafa et al., UNSW-NB15 Dataset.
(3) Nguyen et al., Reinforcement Learning for Cyber Defense.