**RAJALAKSHMI ENGINEERING COLLEGE**

**DEPARTMENT OF ARTIFICIAL INTELLIGENCE & MACHINE LEARNING**

**IV YEAR PROJECT-ABSTARCT (2024-25)**

|  |  |  |
| --- | --- | --- |
| **TITLE** |  | |
| **TEAM MEMBERS** | **Reg. No** | **Name** |
| **PROJECT MENTOR** |  | |
| **PROJECT ID** |  | |

|  |
| --- |
| **ABSTRACT**  The rapid expansion of IoT devices has significantly increased the threat landscape, with botnet attacks emerging as a critical security concern.Traditional detection methods often fail to effectively manage the complexity and volume of IoT traffic, necessitating innovative solutions .This project aims to develop a robust and adaptive detection system by integrating Convolutional Neural Networks (CNNs) with Reinforcement Learning (RL). The customized CNN architecture will be optimized for feature extraction from IoT network traffic, while RL techniques will enhance the model's ability to adaptively improve detection accuracy and response times.By leveraging these advanced machine learning techniques, the proposed system seeks to provide a scalable, real-time solution for effectively detecting and mitigating botnet attacks in IoT environments. The RL component will continuously adapt to new and evolving attack patterns, ensuring the model remains effective over time. This integration promises a significant advancement in IoT security, offering a dynamic and resilient defense against increasingly sophisticated cyber threats. Through rigorous evaluation using real-world datasets and metrics such as accuracy, precision, recall, and F1-score, the project aims to demonstrate the superior performance and practicality of the proposed approach in maintaining the integrity and security of IoT networks. |
|  |

**SUPERVISOR REVIEWER PROJECT CO-ORDINATOR**