Project Proposal

BSAI-V

Fall – 2025

Course:

AI335L-Deep Learning Lab

Course Instructor

Ms. Bismah Malik

Department of Creative Technologies

Faculty of Computing & AI

Air University, Islamabad

Team Members

Sr. No.	Student Name	Registration Number	Role / Contribution
1	Malik Saad Ahmed	231224	Data Handling
2	Muhammad Umar	231200	Documentation
3	Talha Ahmed Siddiqui	231230	Model Development

1. Project Title

Autonomous Network Intrusion Response System using Deep Reinforcement Learning

2. Problem Statement

Modern networks face increasingly sophisticated cyberattacks such as DDoS, brute force, port scans, and botnet intrusions. Traditional intrusion detection systems (IDS) can detect attacks but lack the ability to **respond intelligently** in real time. Current defense approaches rely on static firewall rules or manually configured security policies, which are slow, ineffective against evolving threats, and prone to false alarms. Therefore, there is a need for an **autonomous intrusion response system** that can dynamically learn optimal defense strategies.

This project proposes a **Deep Reinforcement Learning (DRL)-based intrusion response system** that not only detects malicious network activity but also decides the **best response action**, such as blocking malicious IPs, throttling suspicious traffic, or allowing safe connections. The system learns from experience to minimize false positives while maintaining network availability. This approach can improve cybersecurity automation in enterprise, cloud, and IoT networks.

3. Literature Review / Related Work

#	Paper / Source (link)	Year	Approach Used	Dataset	Accuracy / Results	Limitations
1	"Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection" —	2022 ?	Deep Q-Network (DQN) + Deep Feed-Forward Neural Network for intrusion detection. (MDPI)	NSL-KDD	Achieved >90% accuracy in intrusion classification. (MDPI)	Focuses on detection only; lacks response/decision-making phase.

	MDPI. (MDPI) Link					
2	“Network Intrusion Response using Deep Reinforcement Learning in …” — ACM DL. (ACM Digital Library) Link	~2024	Deep RL for intrusion response system (actions to mitigate). (ACM Digital Library)	(Simulated environment)	Demonstrated intrusion response capability using RL.	Possibly limited attack variety, simulation only.
3	“Reinforcement Learning for Intrusion Detection: More Model Longness and Fewer Updates” — IEEE TNSM. (ResearchGate) Link	2022	RL model aimed at reducing model updates, using sliding window & transfer learning. (ResearchGate)	8 TB dataset (real-network traffic)	Reduced false positives up to 8%, false negatives up to 34%, accuracy variation ≤6%. (ResearchGate)	More detection than response; complex dataset makes replication harder.
4	“AI-Driven Dynamic Firewall Optimization Using Reinforcement Learning for Anomaly Detection and Prevention” — arXiv. (arXiv) Link	2025 (pre-print)	Deep RL controlling firewall rules (LSTM-CNN + DRL). (arXiv)	NSL-KDD & CIC-IDS2017 (simulated SDN)	Improved detection accuracy, reduced false positives & rule update latency. (arXiv)	Pre-print (may not be peer-reviewed); response focused but network environment simulated.
5	“A Survey for Deep Reinforcement Learning Based Network Intrusion Detection” — arXiv. (arXiv) Link	2024	Survey of DRL for intrusion detection: reviews architectures, datasets, challenges. (arXiv)	Various public datasets	Provides overview of state-of-the-art; identifies gaps.	Survey only (no new experimental results).

4. Identified Gaps / Research Motivation

Although previous research has made progress in intrusion detection using machine learning and deep learning, there are still notable gaps. Most existing work focuses primarily on identifying malicious traffic rather than taking appropriate response actions after detection. Studies using Deep Reinforcement Learning (DRL) have shown potential, but many are limited to simulated environments, use small datasets, or handle only a narrow range of attack types. Furthermore, few studies have addressed how to balance security with network availability, which leads to unnecessary blocking of legitimate traffic and high false positive rates.

To address these limitations, this project proposes an **autonomous intrusion response system** that uses **Deep Reinforcement Learning (DRL)** to make optimal real-time defense decisions. Unlike traditional rule-based systems, the proposed system learns response strategies over time and adapts to new attack behaviors. It will be trained and evaluated on publicly available datasets such as **CIC-IDS2017**, which contains realistic network traffic, making the solution more practical and applicable to real-world scenarios.

5. Proposed Methodology / Novel Approach

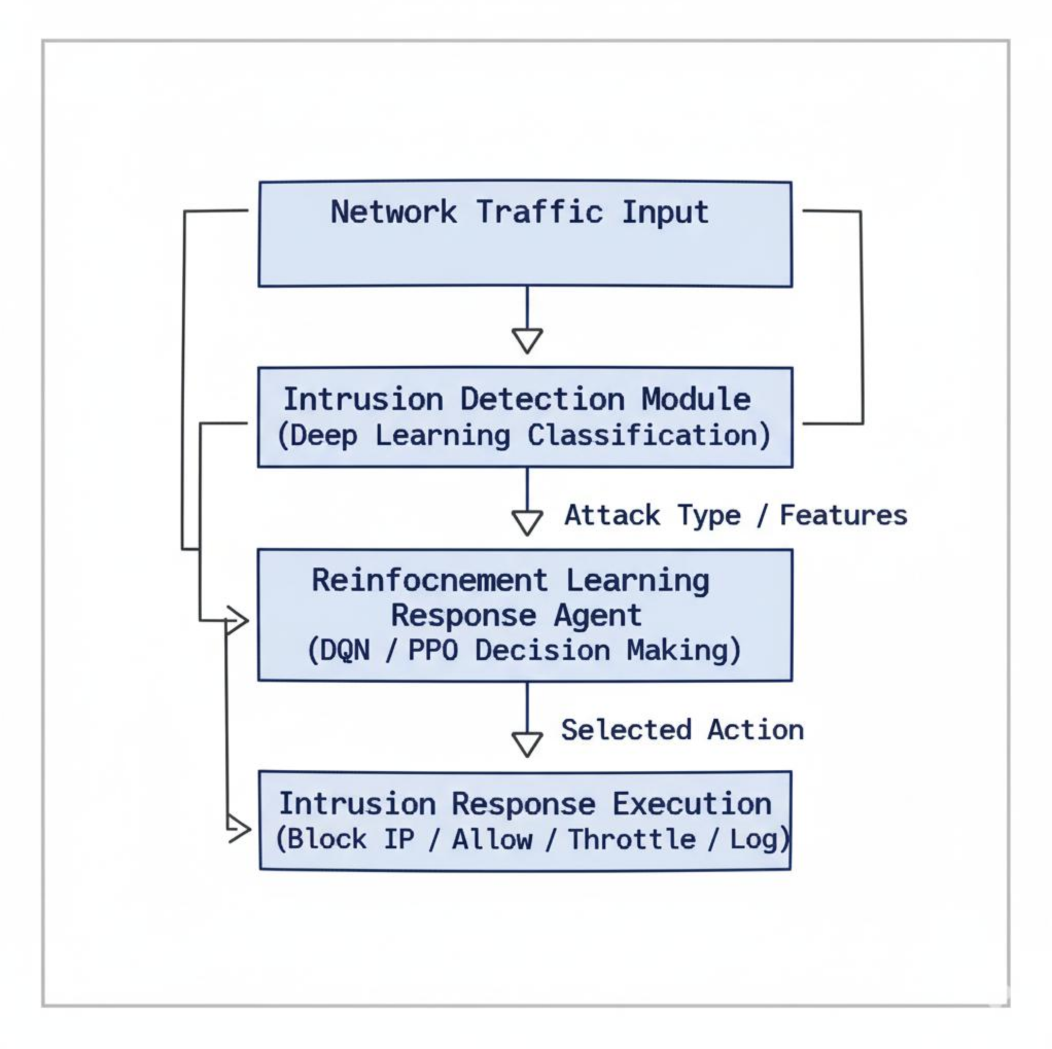
The proposed system will integrate deep learning-based intrusion detection with a Deep Reinforcement Learning (DRL) agent for autonomous response decision-making. The system will operate in two main stages: (1) attack detection and classification, and (2) intelligent response selection.

Step-by-Step Workflow

1. **Data Collection and Preprocessing**
    - Public network traffic datasets (CIC-IDS2017 and NSL-KDD as backup) will be used.
    - The dataset will be cleaned by handling missing values, removing duplicates, and encoding categorical network features.
    - Standardization or normalization will be applied to improve model performance.
2. **Intrusion Detection Module (Deep Learning Model)**
    - A deep neural network (such as an MLP or CNN/LSTM hybrid) will classify incoming network traffic as normal or malicious.
    - This model will serve as a feature extractor for the reinforcement learning stage.
    - The detection model will be trained using supervised learning.
3. **Reinforcement Learning Environment Design**
    - A custom OpenAI Gym-like simulation environment will be created.
    - The **state** will consist of detected attack type, traffic behavior features, and historical actions.
    - The **actions** will include: allow traffic, block source IP, log event only, throttle connection, or isolate host.

- The **reward function** will be designed to minimize false alarms and prevent successful attacks while maintaining network availability.

4. **Deep Reinforcement Learning-Based Response Agent**
   - Two DRL algorithms will be considered: **Deep Q-Network (DQN)** and **Proximal Policy Optimization (PPO)**.
   - The agent will learn an optimal response policy by interacting with the environment.
   - Neural networks will be used inside the DRL models to approximate the policy or Q-value function.
5. **Training and Evaluation**
   - The system will be trained in episodic simulations representing different network attack scenarios.
   - Performance will be evaluated based on response accuracy, attack mitigation rate, false positives, and response time.


Network Traffic Input
Intrusion Detection Module
(Deep Learning Classification)
Attack Type / Features
Reinfocnement Learning
Response Agent
(DQN / PPO Decision Making)
Selected Action
Intrusion Response Execution
(Block IP / Allow / Throttle / Log)

6. Dataset Information

Dataset Name / Source	Type	Size / Samples	Features	Preprocessing Needed
CIC-IDS2017 (Canadian Institute for Cybersecurity)	Network traffic dataset (CSV)	~2.8 million records	80+ flow-based network features such as duration, protocol, packet length, flow rate, etc.	Handling missing values, label encoding, normalization, class imbalance handling
NSL-KDD (backup dataset)	Network connection records	125,973 records	41 features including protocol type, service, flag, source bytes	Categorical encoding, feature scaling, removing duplicates

7. Tools and Technologies

Tool / Technology	Purpose / Usage
Python	Core programming language for implementation
PyTorch / TensorFlow	Deep learning framework for intrusion detection model
Stable Baselines3	Library for implementing Deep Reinforcement Learning algorithms (DQN, PPO)
Gymnasium (OpenAI Gym compatible)	Structure for custom reinforcement learning environment
Pandas & NumPy	Data preprocessing, transformation, and feature handling
Scikit-learn	Feature scaling, encoding, train-test split
Matplotlib / Seaborn	Visualizations and performance plots
Google Colab/VS Code	Model training and GPU environment

8. References

Alavizadeh, H., Jang-Jaccard, J., Singh, A., & Nepal, S. (2022). *Deep Q-learning based reinforcement learning approach for network intrusion detection*. Computers, 11(3), 41. https://doi.org/10.3390/computers11030041

Prasad, K. J. S., & Tripathi, S. (2024). *Network intrusion response using deep reinforcement learning in software-defined networking environments*. Proceedings of the 2024 International Conference on Advanced Computing. ACM. https://doi.org/10.1145/3664476.3670917

Ren, J., Guo, H., Liu, C., Zhao, W., & Li, T. (2022). *Reinforcement learning for intrusion detection: More model longness and fewer updates*. IEEE Transactions on Network and Service Management, 19(4), 3923–3937. https://doi.org/10.1109/TNSM.2022.3207094

Omar, M., Khan, I., Hussain, M., & Abbas, G. (2025). *AI-driven dynamic firewall optimization using reinforcement learning for anomaly detection and prevention*. arXiv preprint. https://arxiv.org/abs/2506.05356

Chamikara, M. A. P., Liu, D., & Jiang, J. (2024). *A survey for deep reinforcement learning-based network intrusion detection*. arXiv preprint. https://arxiv.org/abs/2410.07612