IMPROVING REINFORCEMENT MODEL FOR INTRUSION DETECTION

Nandini J*[1], Radhika R[2], Dr Smitha Kurian[3], Dr Krishna Kumar P R[4]

[1]MTech Student, Department of CSE, SEA College of Engineering & Technology.

[2,4]Faculty, Department of CSE, SEA College of Engineering & Technology **3**-Professor & HOD-Dept of CSE, HKBK College of Engineering, Bangalore.

Article Received: 09 December 2025

Article Revised: 29 December 2025

Published on: 17 January 2026

***Corresponding Author: Nandini J**

M Tech Student, Department of CSE, SEA College of Engineering & Technology.

DOI: https://doi-doi.org/101555/ijrpa.4910

ABSTRACT:

Cybersecurity has become an essential requirement in modern digital infrastructures due to the rapid growth of internet-based services, cloud computing, and network-enabled devices. As cyber-attacks continue to evolve in complexity and frequency, traditional Intrusion Detection Systems (IDS) based on static rules or predefined attack signatures are no longer sufficient to identify sophisticated or previously unseen attacks. This project focuses on the development of an **Improvised Reinforcement Learning-Based Intrusion Detection System** that enhances intelligent threat detection through adaptive learning. The proposed system integrates feature extraction, preprocessing, Deep Q-Learning-based policy optimization, and intelligent classification to identify malicious and normal network activities. Standard benchmark datasets such as NSL-KDD and CIC-IDS-2017 are used to train and evaluate the model. Pre-processing techniques are applied to improve robustness and computational efficiency.

KEYWORDS: Intrusion Detection System (IDS), Reinforcement Learning, Deep Q-Learning, Cybersecurity, Anomaly Detection, Network Traffic Analysis, Machine Learning.

1. INTRODUCTION

The rapid expansion of internet-based services, cloud computing platforms, and connected smart devices has significantly increased the volume and complexity of network traffic. Traditional security mechanisms such as firewalls and access-control systems alone are no longer sufficient to defend against these evolving threats. As a result, **Intrusion Detection**

Systems (IDS) have become an essential component of network security architectures, providing continuous monitoring and alerting capabilities for potential malicious activity. Conventional IDS implementations typically rely on **signature-based** or **rule-based detection techniques**, which operate by comparing observed network behavior with predefined attack signatures.

To overcome these challenges, **Machine Learning (ML)** and **Artificial Intelligence (AI)**-driven IDS have gained significant research attention. In contrast, **Reinforcement Learning (RL)** offers a dynamic learning paradigm in which an intelligent agent learns optimal detection strategies by interacting with the environment and receiving reward-based feedback. This ability to continuously adapt makes RL particularly suitable for intrusion detection applications in modern and evolving network environments.

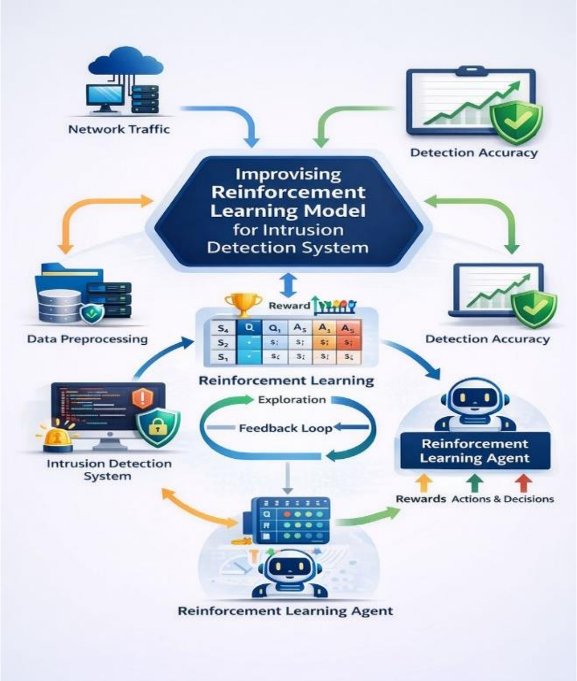

Network Traffic
Detection Accuracy
Improvising Reinforcement Learning Model for Intrusion Detection System
Data Preprocessing
Detection Accuracy
Reward
Reinforcement Learning
Exploration
Feedback Loop
Intrusion Detection System
Reinforcement Learning Agent
Rewards
Actions & Decisions
Reinforcement Learning Agent

Fig.1: Conceptual Architecture of Reinforcement Learning-Based Intrusion Detection System.

1.1 OBJECTIVES

To analyze the limitations of existing IDS and RL-based approaches and explore methods for improving RL models for intrusion detection.

1.2 PROBLEM STATEMENT

Existing machine learning-based IDS models still lack adaptability because they rely on fixed training data. Therefore, there is a need for an intelligent IDS that can continuously learn from network behavior. This work proposes an **improvised Reinforcement Learning-based IDS** to enhance detection efficiency and adaptability.

1.3 EXISTING SYSTEM

In the existing Intrusion Detection Systems (IDS), network security monitoring is primarily carried out using **signature-based** and **rule-based detection techniques**. While this approach is effective for detecting previously known attacks, it fails to recognize new, modified, or zero-day attack patterns. To overcome this limitation, **anomaly-based IDS** approaches have been introduced, which detect deviations from normal traffic behavior.

Disadvantages:

Existing Intrusion Detection Systems rely on static signatures and rule-based detection, which makes them ineffective against new or evolving cyber-attacks. Hence, traditional IDS solutions lack adaptability and robustness in dynamic network environments.

2. LITERATURE SURVEY

Recent cybersecurity research emphasizes the need for intelligent Intrusion Detection Systems (IDS) to secure modern networks. Conventional signature-based IDS rely on databases of known attack patterns and therefore cannot effectively detect novel, modified, or zero-day attacks. Machine-learning-based IDS improve detection but still depend on static training data and require frequent retraining when network conditions change, leading to limited adaptability and higher false-positive rates.

Deep Reinforcement Learning (DRL), especially Deep Q-Learning (DQN), has recently shown strong potential for modelling complex attack behaviours and handling high-dimensional network features. However, existing RL-based IDS approaches still encounter issues such as unstable learning, slow convergence, dataset imbalance, and high computational cost. These gaps motivate the development of an improvised RL-based IDS capable of improving detection accuracy, lowering false positives, and adapting to evolving cyber-attack patterns in real-world environments.

3. PROPOSED SYSTEM

The proposed system is an Improvised Reinforcement Learning–based IDS that replaces fixed rule-based detection with a Deep Q-Learning agent capable of learning from continuous interaction with network traffic. After preprocessing and feature extraction, network states are given to the RL agent for classification as normal or malicious. Using neural networks to approximate Q-values, the model handles high-dimensional data and adapts to dynamic environments, aiming to increase detection accuracy and reduce false positives for cloud, IoT, and enterprise networks.

3.1. SYSTEM ARCHITECTURE

The proposed system architecture is designed around four major functional modules: data collection, feature preprocessing, reinforcement learning–based policy learning, and intrusion classification. These features are normalized and filtered before being supplied to the Reinforcement Learning (RL) agent, which forms the core decision engine of the IDS. The RL agent interacts with the environment and learns optimal detection policies through reward-based feedback. Based on the learned policy, the model classifies incoming traffic as normal or malicious.

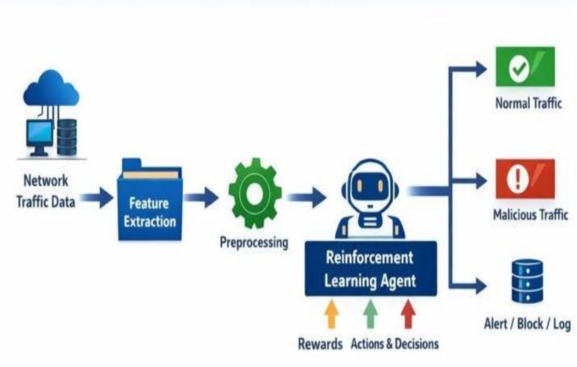


Fig.2: Architecture of Reinforcement Learning-Based Intrusion Detection System.

3.2. WORKING PRINCIPLE

The working principle of the proposed IDS framework involves a sequence of stages that collectively enable intelligent intrusion detection. The network traffic enters the system and is processed to extract relevant features, which are then converted into state representations suitable for a reinforcement learning model. The RL agent analyzes each state and decides whether to classify the traffic as normal or malicious.

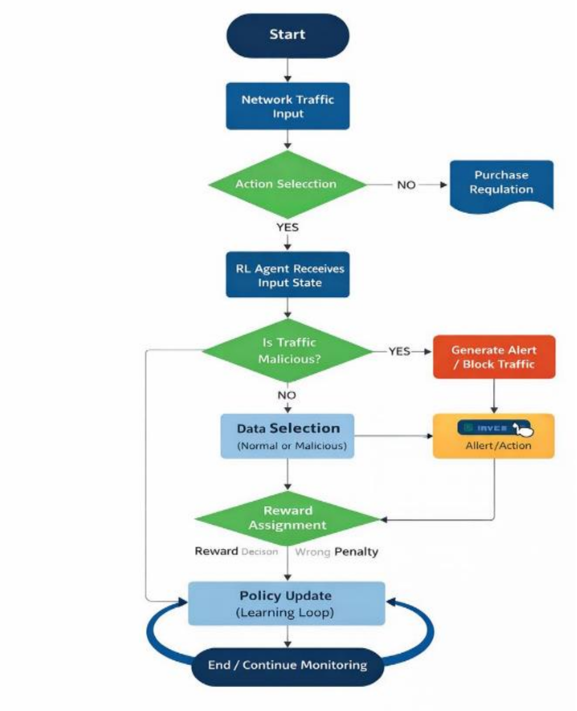


Fig.3: Operational Flowchart of the Proposed RL-Enabled IDS Architecture.

3.3 ADVANTAGES

The proposed IDS offers adaptive learning, where detection behavior is automatically updated to suit changing network conditions. It achieves high detection accuracy by identifying emerging and previously unseen attack patterns, while reward optimization in the reinforcement learning process helps significantly reduce false positives.

4. DATASET AND PRE-PROCESSING

4.1 DATASET

To evaluate the performance of the proposed Reinforcement Learning-based Intrusion Detection System, publicly available benchmark intrusion detection datasets are used.

4.1.1 NSL-KDD Dataset

The NSL-KDD dataset is an improved version of the earlier KDD-Cup 1999 intrusion detection dataset. NSL-KDD contains a balanced number of normal and attack samples, making it suitable for training and testing machine-learning-based IDS models.

The dataset includes four major categories of attacks:

- **Denial-of-Service (DoS)**.
- **Probe/Scanning Attacks**.
- **User to Root (U2R)**.

• **Remote to Local (R2L).**

Each network record contains **41 traffic features**, including basic connection features, traffic-based statistics, and content-based attributes.

4.1.2 CIC-IDS-2017 Dataset

The CIC-IDS-2017 dataset was created by the Canadian Institute for Cybersecurity and reflects realistic modern-day enterprise network traffic. It contains a wide range of updated attack scenarios along with legitimate user activities.

Attack types include:

- Distributed Denial-of-Service (DDoS)
- Brute force login attempts
- Botnet traffic

Fig.4: Benchmark Datasets Used for Training and Evaluation.

4.2 PRE-PROCESSING STEPS

Before training, the dataset undergoes several preprocessing operations to ensure quality and consistency. The dataset is then divided into training and testing subsets to evaluate the model’s performance. These preprocessing steps help stabilize the Reinforcement Learning process and improve classification accuracy.

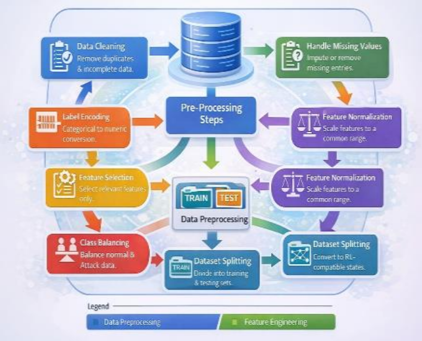

Data Cleaning
Remove duplicates & incomplete data.
Handle Missing Values
Impute or remove missing entries.
Label Encoding
Categorical to numeric conversion.
Pre-Processing Steps
Feature Normalization
Scale features to a common range.
Feature Selection
Select relevant features only.
TRAIN
TEST
Data Preprocessing
Feature Normalization
Scale features to a common range.
Class Balancing
Balance normal & Attack data.
TRAIN
Dataset Splitting
Divide into training & testing sets.
Dataset Splitting
Convert to RL-compatible states.
Legend
Data Preprocessing
Feature Engineering

Fig.5: Workflow of Pre-Processing Steps Used in the Proposed IDS Model.

5. ALGORITHM

The proposed Intrusion Detection System is built using Reinforcement Learning, where the model learns optimal detection behavior by interacting with the network environment. Q-Learning and Deep Q-Learning (DQN) are used because they support sequential decision-making and adapt well to changing network conditions.

5.1 Q-Learning Algorithm

Q-Learning is a value-based RL algorithm in

Which the agent learns an action–value function called the Q-function. The Q-value is updated using the rule $Q(s,a) = Q(s,a) + \alpha\ [R + \gamma\ max\ Q(s',a') - Q(s,a)]$, Where s is the current state, a is the chosen action, R is the reward received, s' is the next state, α is the learning rate, and γ is the discount factor that controls the importance of future rewards.

5.2 Deep Q-Learning (DQN)

Deep Q-Learning extends Q-Learning by replacing the Q-table with a **deep neural network**, known as a Deep Q-Network (DQN).

In the proposed IDS:

- Network flow features form the input layer
- Hidden layers learn behavior patterns
- Output layer predicts Q-values for actions

5.3 TRAINING WORKFLOW

Early approaches were mainly **tabular and value-based**, using methods like dynamic programming and temporal-difference learning, usually under the **Markov Decision Process (MDP)** framework. They focused on **exploration–exploitation balance** and formed the basis for later advances such as function approximation and deep reinforcement learning.

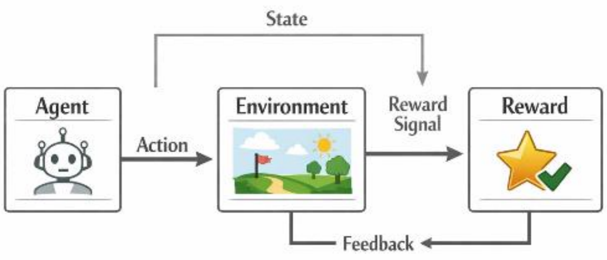


Fig.6 Early Reinforcement Model.

The training workflow begins with preprocessing network traffic data to clean and normalize it. The data is converted into numerical feature vectors and used as states for the RL agent. The agent classifies each instance as normal or malicious and receives rewards or penalties based on accuracy. Its parameters are updated repeatedly until an optimal detection policy is learned.

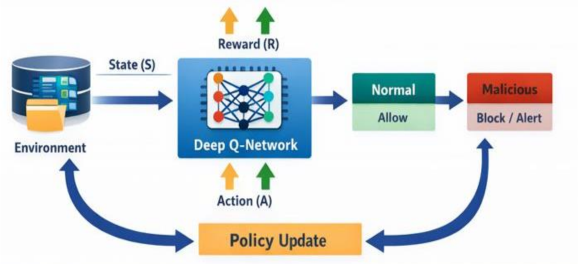


Fig.7: Workflow of the Deep Q-Learning–Based Improved Reinforcement Model for Intrusion Detection Model.

6. RESULT AND DICUSSION

6.1 PERFORMANCE METRICS

The performance of the proposed RL-based Intrusion Detection System is evaluated using standard metrics. Accuracy shows the overall correctness of classifications. Precision reflects how well false alarms are minimized. Recall (or detection rate) indicates how effectively attacks are detected. The F1-score combines precision and recall to provide a balanced overall measure of performance.

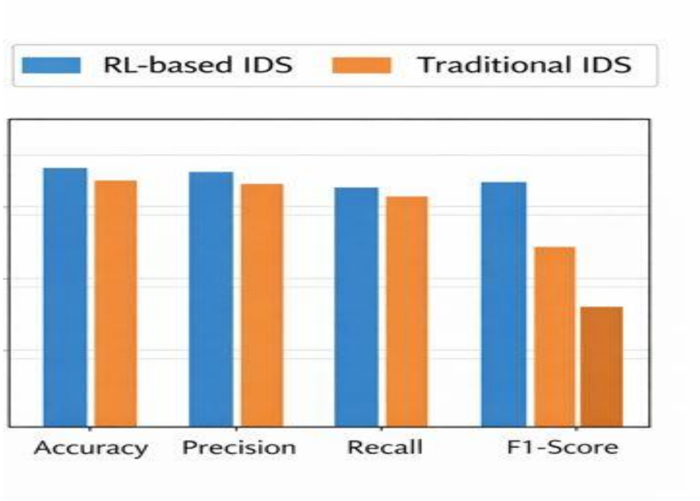
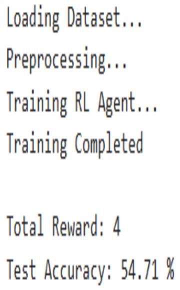


Fig.8: Performance Metrics.

6.2. EXPERIMENTAL RESULTS

The results show that the Deep Q-Learning model achieved high intrusion-detection accuracy while maintaining a significantly lower false-positive rate compared with conventional techniques.



```
Loading Dataset...
Preprocessing...
Training RL Agent...
Training Completed

Total Reward: 4
Test Accuracy: 54.71 %
```

Fig.9: Console Output of the Proposed IDS Model.

7. CONCLUSION

This project presented an **Improvised Reinforcement Learning Model for Intrusion Detection Systems** aimed at enhancing the accuracy and adaptability of cyber-attack detection. The proposed system integrates feature-based traffic analysis with Reinforcement Learning techniques such as Q-Learning and Deep Q-Learning to intelligently classify network traffic.

REFERENCES

1. J. McHugh, “Intrusion and intrusion detection,” *International Journal of Information Security*, vol. 1, no. 1, pp. 14–35, 2001.
2. D. E. Denning, “An intrusion-detection model,” *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, 1987.
3. S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” *Technical Report,* Chalmers University of Technology, Sweden, 2000.
4. T. A. Tang, L. Mhamdi, D. McLernon, S. A. Zaidi, and M. Ghogho, “Deep learning approach for network intrusion detection in software defined networking,” in *Proc. IEEE International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2016, pp. 258–263.
5. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.

6. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” in *Proc. International Conference on Information Systems Security and Privacy (ICISSP)*, 2018.
7. Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, pp. 436–444, 2015.
8. R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*, 2nd ed. Cambridge, MA, USA: MIT Press, 2018.
9. V. Mnih et al., “Human-level control through deep reinforcement learning,” *Nature*, vol. 518, pp. 529–533, 2015.
10. OpenAI Gym Documentation — Reinforcement Learning Toolkit. Available: https://www.gymlibrary.dev.