iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83995

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

An Intelligent Network Intrusion Detection System Using Deep Reinforcement Learning

Sana Fathima[1], O. B. V. Ramanaiah[2]
[1]*M. Tech Student of Department of Computer Science and Engineering, JNTU Hyderabad, Telangana, India*
[2]*Senior Professor of the Department of Computer Science and Engineering, JNTU Hyderabad, Telangana, India*

Abstract: ***Cyberattacks continue to threaten computer networks and information systems, making effective intrusion detection more important than ever. While traditional machine learning and deep learning-based Intrusion Detection Systems (IDS) have achieved encouraging results, they often face challenges in accurately identifying multiple types of attacks with low false alarms. To address this limitation, this study presents a Deep Reinforcement Learning (DRL)-based IDS that uses the Deep Q-Network (DQN) algorithm for multiclass network attack detection. The proposed system classifies network traffic into five categories: Normal, Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). The NSL-KDD dataset was used for training and evaluation, and class imbalance was addressed using the Synthetic Minority Oversampling Technique (SMOTE). The performance of the DQN model was compared against three distinct machine learning paradigms: a supervised Multilayer Perceptron (MLP), an unsupervised Autoencoder, and an ensemble Voting Classifier. The experimental results show that the DQN-based IDS outperformed the other models, achieving 97.96% accuracy, 98.70% precision, 97.96% recall, and an F1-score of 98.24%, along with a low false positive rate of 0.33%. These findings demonstrate that deep reinforcement learning can significantly enhance multiclass intrusion detection while reducing false alarms, making it a promising approach for strengthening network security.***

Keywords: ***Intrusion Detection System, Deep Reinforcement Learning, Deep Q-Network, Network Security, NSL-KDD, Multiclass Classification.***

I. INTRODUCTION

The rapid expansion of computer networks and internet-based services has significantly increased the exposure of organisational and personal information systems to cyber threats. Cyberattacks can lead to serious consequences, including data breaches, service disruptions, financial losses, and unauthorised access to sensitive information. To mitigate these risks, Intrusion Detection Systems (IDS) have become a fundamental component of modern network security frameworks. IDS monitor network traffic and identifies suspicious or malicious activities, thereby helping to protect computer networks from a wide range of cyber threats. Recent studies have confirmed their effectiveness in strengthening network security [1], [3].

Machine learning and deep learning techniques have been extensively applied to enhance the performance of intrusion detection systems. Various approaches, including hybrid machine learning models, deep neural networks, and optimisation-based techniques, have reported promising results in detecting network intrusions [1], [5], [6]. However, despite these advancements, many existing methods rely on static learning mechanisms. As cyber threats continue to evolve in complexity and diversity, such approaches may struggle to adapt to new attack patterns while maintaining high detection accuracy and low false positive rates.

To address these challenges, researchers have increasingly explored Deep Reinforcement Learning (DRL) for intrusion detection. Unlike conventional supervised learning methods, DRL enables models to learn adaptive decision-making strategies through continuous interaction with their environment. Recent studies have demonstrated that reinforcement learning can enhance the adaptability and performance of intrusion detection systems in dynamic network environments [10], [11], [12]. Among DRL techniques, the Deep Q-Network (DQN) algorithm integrates reinforcement learning with deep neural networks, allowing it to effectively handle complex state spaces and making it a promising solution for multiclass intrusion detection tasks.

Motivated by the potential of DRL-based approaches, this paper proposes a DQN-based intrusion detection system for multiclass network attack classification using the NSL-KDD dataset. The proposed model categorises network traffic into five classes: Normal, Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). To comprehensively evaluate the effectiveness of the proposed approach, the performance of the DQN model is compared against baseline models representing three major machine learning paradigms: supervised learning (Multilayer Perceptron - MLP), unsupervised learning (Autoencoder), and ensemble learning (Voting Classifier).

The main contributions of this work are as follows:

- Development of a DQN-based intrusion detection system for multiclass network attack classification.
- Comparative evaluation of DQN against supervised, unsupervised, and ensemble learning models using the NSL-KDD dataset.
- Demonstration of improved detection performance and reduced false positive rates achieved by the proposed DQN model.

The remainder of this paper is organised as follows. Section II reviews related work on intrusion detection systems. Section III presents the proposed methodology and experimental setup. Section IV discusses the experimental results and performance evaluation. Finally, Section V concludes the paper and outlines future research directions.

II. RELATED WORK

Recent research has extensively explored machine learning and deep learning techniques to enhance intrusion detection performance. For instance, Wisanwanichthan and Thammawichai [1] proposed a double-layered hybrid framework combining Naive Bayes and Support Vector Machine classifiers to improve detection accuracy. Similarly, Abrar et al. [2] demonstrated the effectiveness of data-driven machine learning approaches on the NSL-KDD dataset. Muhammad et al. [4] introduced a stacked Autoencoder and Deep Neural Network-based intrusion detection system that learned compact feature representations and achieved strong multiclass classification performance across multiple intrusion detection datasets. Advancing this direction, Gupta et al. [5] introduced a hybrid optimisation and deep learning-based IDS, while Hnamte and Hussain [6] developed a hybrid DCNN-BiLSTM model. These studies reported promising detection performance; however, most of the proposed approaches rely on supervised learning mechanisms, and their performance depends heavily on the quality and distribution of the training data.

To further boost prediction stability and accuracy, ensemble learning has been widely investigated as a means of combining multiple classifiers. Seth et al. [7] designed an ensemble framework integrating diverse learning algorithms to enhance both accuracy and robustness. In a similar vein, Arreche et al. [8] presented a two-level ensemble framework that outperformed individual classifiers in network intrusion detection. Additionally, Sidharth and Kavitha [9] utilised stacking and boosting techniques to strengthen attack classification capabilities. Although ensemble approaches can improve classification performance by combining the strengths of multiple learning algorithms, they are generally trained using fixed datasets and predefined learning models.

To address the limitations of conventional learning approaches, researchers have increasingly explored reinforcement learning (RL) and DRL for intrusion detection. Lopez-Martin et al. [11] demonstrated that DRL can effectively learn attack detection strategies directly from network traffic data. Building on this, Alavizadeh et al. [12] proposed a Deep Q-Learning-based approach that yielded encouraging results for network attack classification. Gulmez and Angin [13] further investigated the effectiveness of deep reinforcement learning for intrusion detection and highlighted its potential for adaptive decision-making. More recently, Hossain [10] introduced a Deep Q-Learning Intrusion Detection System (DQ-IDS) to create a self-learning cybersecurity framework. Extending this line of research, Badr [14] applied Dueling Double Deep Q-Learning to IDS, while Hsu and Matsuoka [15] proposed a DRL-based anomaly detection framework tailored for network security.

While the literature clearly demonstrates a growing interest in applying reinforcement learning to network security, achieving effective multiclass attack classification while simultaneously maintaining high detection accuracy and low false positive rates remains a significant challenge. Furthermore, many existing studies lack a comprehensive comparison across different learning paradigms. Motivated by these gaps, this work proposes a DQN-based intrusion detection system and conducts a rigorous comparative evaluation against baseline models representing three major machine learning paradigms: supervised learning (MLP), unsupervised learning (Autoencoder), and ensemble learning (Voting Classifier) using the NSL-KDD dataset.

III. METHODOLOGY

This section presents the methodology used for developing the proposed intrusion detection system. It includes the overall system architecture, dataset description, data preprocessing techniques, DQN-based intrusion detection model, comparative models, and experimental setup used for performance evaluation.

A. Overview of the Proposed System

The overall architecture of the proposed intrusion detection system is shown in Figure 1. The system is designed to classify network traffic into multiple attack categories using DRL and comparative machine learning models. The implementation consists of data preprocessing, model training and testing, and performance evaluation stages.

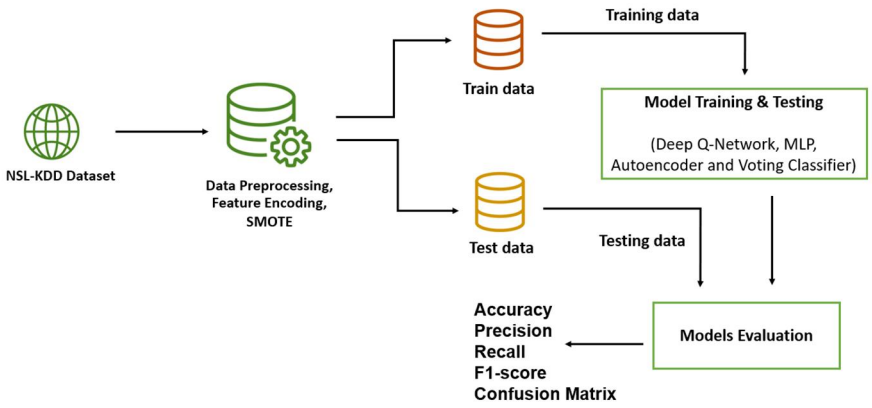


Fig. 1: System Architecture

The process begins with the NSL-KDD dataset. During the preprocessing stage, categorical features are converted into numerical values, and SMOTE is applied to resolve class imbalance issues. Once cleaned, the data is split into training and testing sets.
The training set is used to build the proposed DQN alongside three baseline models representing different learning paradigms: a supervised MLP, an unsupervised Autoencoder, and an ensemble Voting Classifier. Once trained, these models are evaluated on the testing set to assess how well they classify network attacks.
Finally, the models categorise the network traffic into five distinct classes: Normal, DoS, Probe, R2L, and U2R. Performance evaluation is performed using metrics such as accuracy, precision, recall, F1-score, and false positive rate, supplemented by confusion matrix analysis. This comprehensive evaluation allows for a direct and fair comparison between the proposed DQN model and the implemented comparative models.

B. Dataset Description

This work relies on the NSL-KDD dataset for both training and evaluation. It is an improved version of the original KDD Cup 1999 dataset, and it remains a standard choice in security research because it removes duplicate records, giving a much fairer baseline for evaluation [16]. Each network connection in the dataset is described by 41 different features, covering everything from basic protocol details and service attributes to broader traffic behaviour.
Because this is a multiclass classification task, the specific attack records were grouped into four main categories: DoS, Probe, R2L, and U2R. Along with normal traffic, these form the five target classes the proposed system is designed to predict.

C. Data Preprocessing

Data preprocessing was performed to prepare the NSL-KDD dataset for model training and evaluation. Initially, the attack labels were grouped into four major attack categories: DoS, Probe, R2L, and U2R, along with normal network traffic, as shown in Table I. This grouping enabled multiclass attack classification using five target classes.

TABLE I
ATTACK CATEGORISATION IN NSL-KDD DATASET

Attack Category	Attack Types
DoS	back, land, neptune, pod, smurf, teardrop
R2L	guess_passwd, imap, ftp_write, multihop, phf, spy, warezclient, warezmaster
Probe	ipsweep, nmap, portsweep, satan
U2R	buffer_overflow, loadmodule, perl, rootkit
Normal	normal

Because the dataset contains a mix of numerical and categorical features, the categorical attributes were converted into numbers using label encoding. The attack labels were similarly encoded into numerical values. The "difficulty level" column was also dropped, as it is not a realistic input feature for real-world intrusion detection.

Once the data was encoded, it was split into training and testing sets at an 80:20 ratio. For the MLP and Autoencoder models, a portion of the training data was set aside as a validation set to monitor performance and prevent overfitting during training. Finally, Min-Max normalisation was applied to scale all features into a common range, ensuring the models could train effectively.

The NSL-KDD dataset exhibits class imbalance, particularly for the R2L and U2R attack categories, as illustrated in Figure 2. To address this issue, the Synthetic Minority Oversampling Technique (SMOTE) was applied to the training data to generate synthetic samples for minority classes and improve class distribution balance [17]. The preprocessed dataset was subsequently used for training and evaluating the DQN, MLP, Autoencoder, and Voting Classifier models.

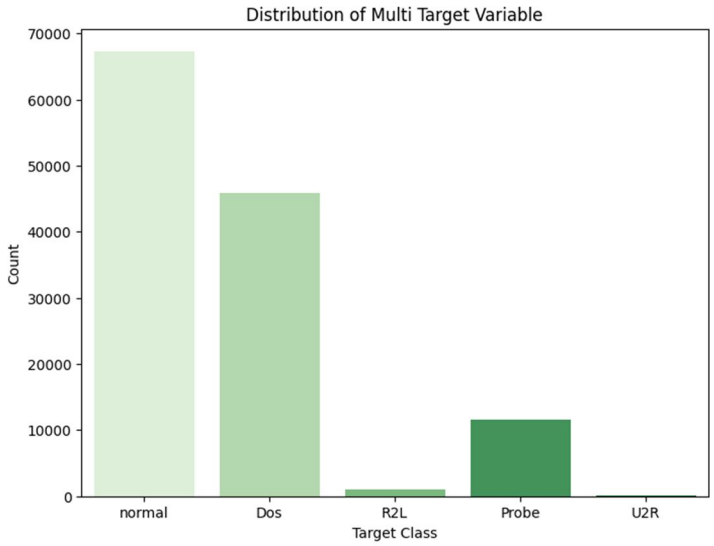


Fig. 2: Distribution of Attack Categories

D. Proposed DQN-Based IDS

The architecture of the proposed DQN-based intrusion detection system is shown in Figure 3. The implementation is based on the DQN algorithm, which combines reinforcement learning with deep neural networks to learn effective decision-making policies [18]. The objective of the model is to classify network traffic into five categories: Normal, DoS, Probe, R2L, and U2R.

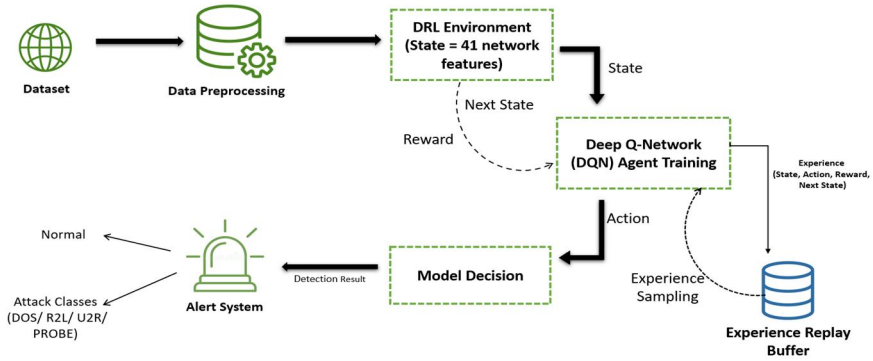


Fig. 3: Proposed DQN-Based IDS Architecture

In the proposed implementation, each network traffic record in the NSL-KDD dataset is represented by 41 input features and treated as a state for the DQN agent. Based on the observed state, the agent predicts an action corresponding to one of the five traffic categories. During training, rewards are assigned according to whether the predicted attack class is correct. Correct classifications receive positive rewards, whereas incorrect classifications receive penalties. The interaction information, including state, action, reward, and next state, is stored in an experience replay buffer and used to update the DQN model.

E. Comparative Models

To evaluate the effectiveness of the proposed DQN model, three comparative models were implemented using the same preprocessed dataset and evaluation framework.

1) *Multilayer Perceptron (MLP):* The MLP model was implemented as a supervised deep learning classifier for multiclass intrusion detection. It is built from multiple fully connected hidden layers with ReLU activation functions, along with batch normalisation and dropout to reduce overfitting. The output layer predicts one of the five traffic categories: Normal, DoS, Probe, R2L, or U2R.
2) *Autoencoder:* An autoencoder-based classification model was implemented to learn compressed feature representations from the network traffic data. The model is made up of three components: an encoder, a decoder, and a classification head. During training, it performs feature reconstruction and multiclass attack classification at the same time, using a combined reconstruction and classification loss. The output layer predicts the same five traffic categories used throughout this study.
3) *Voting Classifier:* The Voting Classifier was implemented as an ensemble approach that combines Random Forest and Logistic Regression. Soft voting was used, meaning the class probability estimates from the individual classifiers are aggregated to produce the final prediction. The ensemble model was used to evaluate the effectiveness of combining multiple learning algorithms for intrusion detection.

F. Experimental Setup

All experiments were carried out on the preprocessed NSL-KDD dataset. To ensure a fair comparison, the DQN, MLP, Autoencoder, and Voting Classifier models were all trained and evaluated under the same experimental framework. Performance was measured using accuracy, precision, recall, and F1-score.

Table II presents the hyperparameter configuration used to train the proposed DQN model.

TABLE II
DQN HYPERPARAMETER CONFIGURATION

Hyperparameter	Value
Hidden Dimension	64
Learning Rate	0.0003
Discount Factor (γ)	0.95
Replay Buffer Capacity	50,000
Batch Size	256
Initial Epsilon	1.0
Minimum Epsilon	0.1
Epsilon Decay Steps	40,000
Target Network Update Frequency	1,000 Steps
Training Steps	50,000

For the comparative models, the MLP was trained with stochastic gradient descent at a learning rate of 0.001, with early stopping applied to prevent overfitting. The Autoencoder used an encoding dimension of 20 and a learning rate of 0.0005, also with early stopping during training. The Voting Classifier combined Random Forest and Logistic Regression, using a soft voting strategy to produce the final prediction.

IV. EXPERIMENTAL RESULTS

The performance of the proposed DQN-based intrusion detection system was evaluated on the NSL-KDD dataset and compared with three benchmark models: MLP, Autoencoder, and Voting Classifier. The objective of this study was to develop an effective multiclass intrusion detection model capable of accurately classifying network traffic into five categories: Normal, DoS, Probe, R2L, and U2R, while maintaining a low false positive rate. Performance was assessed using accuracy, precision, recall, F1-score, and false positive rate (FPR), supported by confusion matrix analysis.

Table III and Figure 4 present the overall performance comparison of the evaluated models. The proposed DQN model performed best across all evaluation metrics, reaching an accuracy of 97.96%, precision of 98.70%, recall of 97.96%, and an F1-score of 98.24%. In comparison, the MLP achieved an accuracy of 95.52%, followed by the Autoencoder at 94.51% and the Voting Classifier at 93.09%. These results suggest that the DQN-based approach was better at learning the complex patterns in network traffic and distinguishing between the different attack categories.

TABLE III
PERFORMANCE COMPARISON OF MODELS

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DQN	97.96	98.70	97.96	98.24
MLP	95.52	97.48	95.52	96.31
Autoencoder	94.51	97.24	94.51	95.66
Voting Classifier	93.09	95.99	93.09	94.16

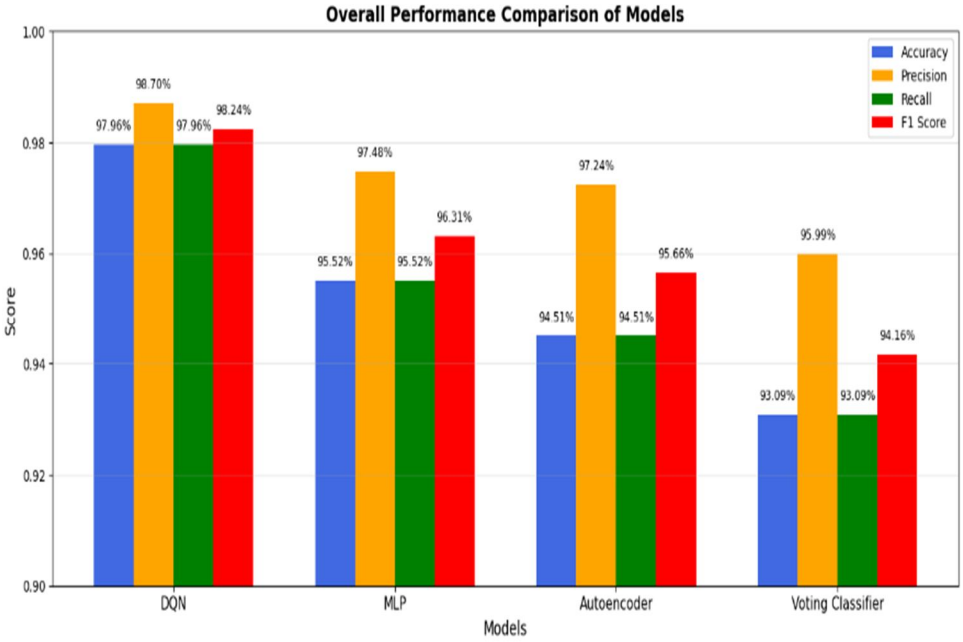


Fig. 4: Overall Performance Comparison of Models

The stronger performance of the DQN model can be explained by its reinforcement learning framework, which allows the agent to learn decision-making policies through reward-based interactions. Because the model continuously updates its policy based on classification outcomes, it was able to refine its attack detection behaviour over time and generalise better across the different attack categories.

Figure 5 shows the confusion matrix of the DQN model. Most network traffic records were correctly classified, with particularly high detection performance for the Normal, DoS, and Probe categories. The minority classes, R2L and U2R, were also handled reasonably well. While a small number of misclassifications occurred, mainly among the minority attack categories, the overall results demonstrate that the DQN model can handle multiclass intrusion detection effectively. Notably, the model maintained strong predictive performance across all classes despite the inherent class imbalance in the NSL-KDD dataset.

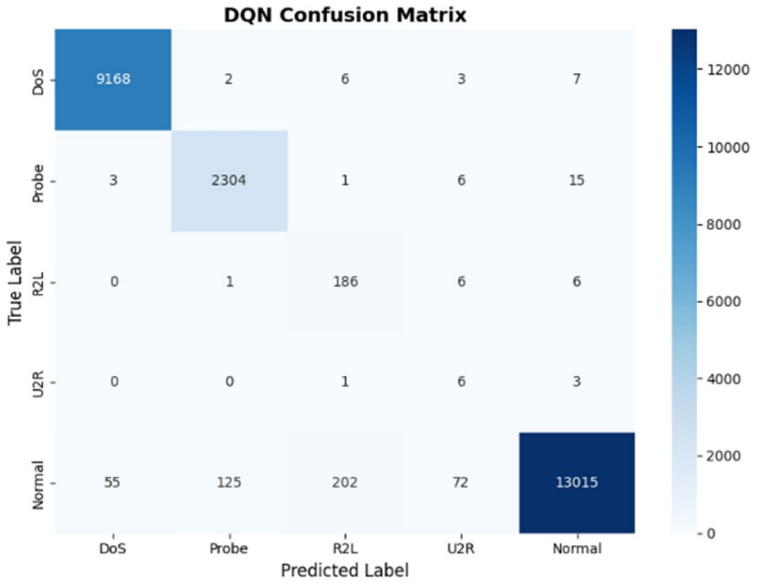


Fig. 5: DQN Model Confusion Matrix

The false positive rate comparison is shown in Figure 6. The proposed DQN model achieved the lowest FPR at 0.33%, outperforming the MLP (1.33%), Autoencoder (1.36%), and Voting Classifier (1.48%). This matters in practice: in real intrusion detection deployments, excessive false alarms can overwhelm security analysts and reduce operational efficiency. The low false positive rate achieved by the DQN model shows that it can reliably separate normal traffic from malicious activity while keeping incorrect alerts to a minimum.

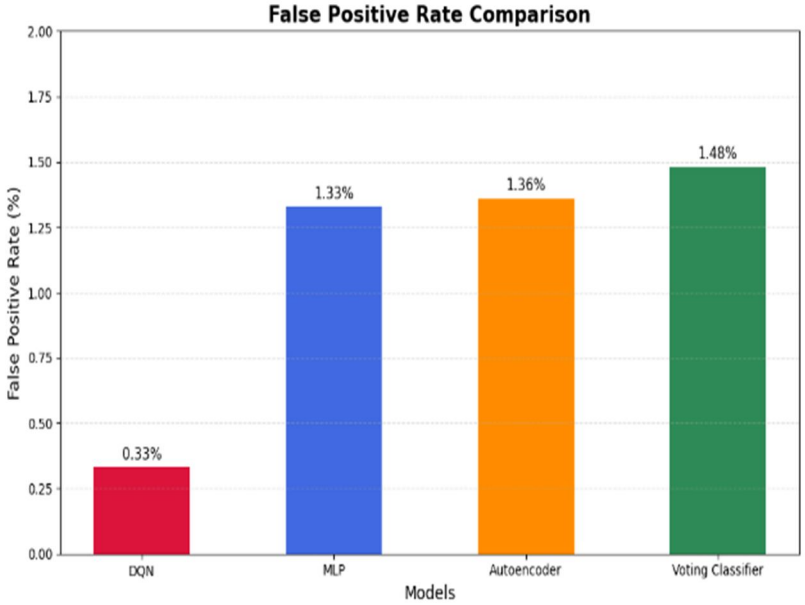


Fig. 6: False Positive Rate Comparison of Models

The training behaviour of the DQN model is illustrated in Figures 7 and 8. Figure 7 shows the loss trend during training, where the loss decreases steadily and then stabilises, indicating that the model learned successfully and converged. Figure 8 presents the exploration–exploitation balance through epsilon decay. Early in training, the agent explores extensively to learn the different attack patterns in the environment. As training progresses, the exploration rate gradually drops, allowing the agent to rely more on the policy it has learned. This smooth shift from exploration to exploitation contributed to the stable performance of the final model.

Fig. 7: DQN Loss Trend Over Training

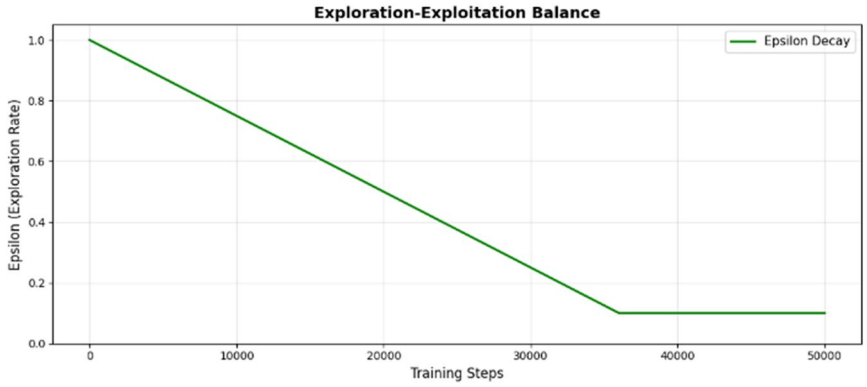


Fig. 8: Exploration–Exploitation Balance During Training

Overall, the experimental results confirm that the proposed DQN-based intrusion detection system met the objectives of this study. The model not only delivered the highest accuracy, precision, recall, and F1-score among all the evaluated approaches, but also achieved the lowest false positive rate. Taken together, these findings indicate that deep reinforcement learning is an effective approach for multiclass intrusion detection and can offer real improvements in attack classification for network security applications.

V. CONCLUSION AND FUTURE WORK

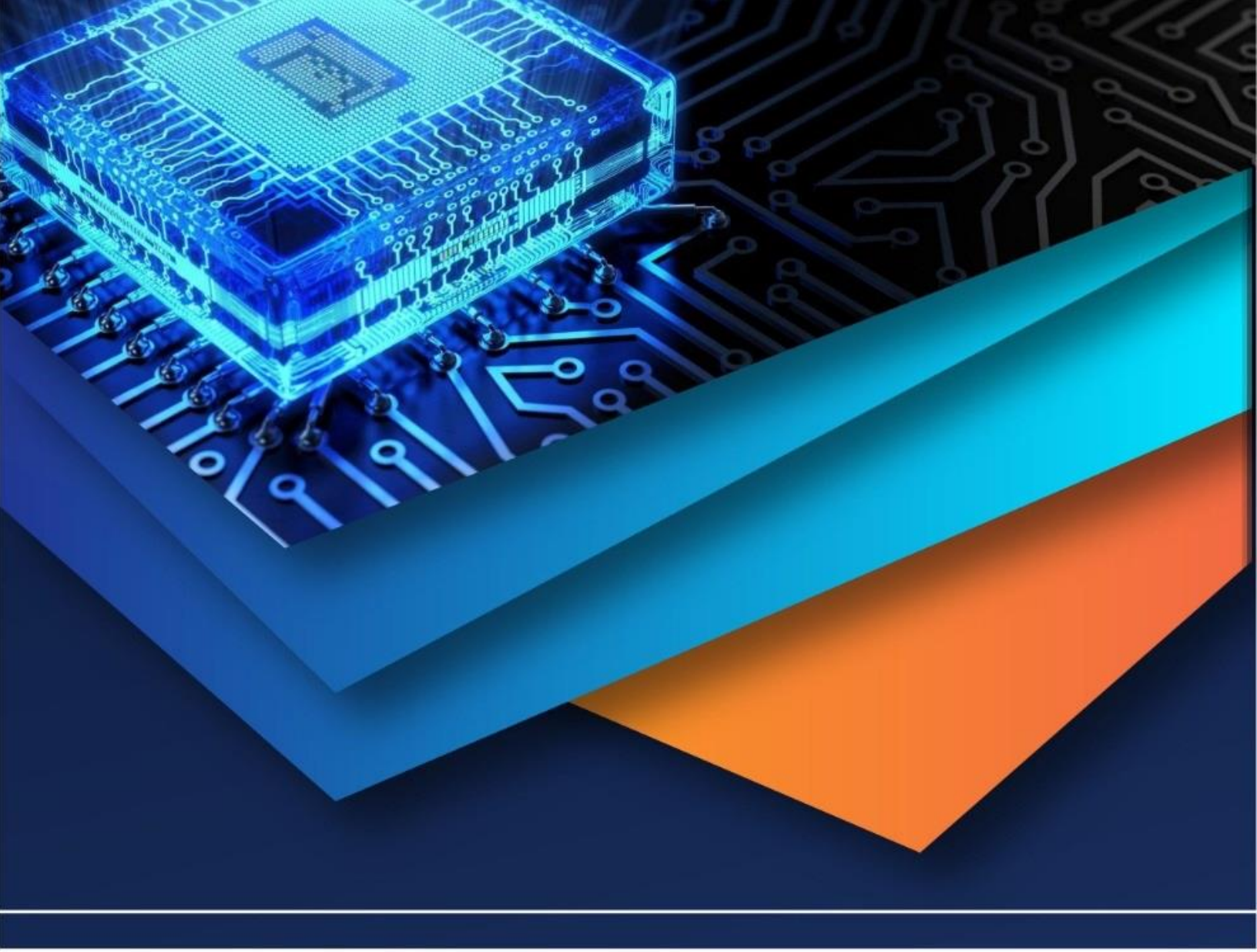
This study presented a Deep Q-Network (DQN)-based intrusion detection system for multiclass network attack classification. The approach was designed to accurately identify Normal, DoS, Probe, R2L, and U2R traffic while keeping false alarms to a minimum. In the experimental evaluation, the DQN model consistently outperformed the MLP, Autoencoder, and Voting Classifier models across all evaluation metrics. These results suggest that the reward-driven learning mechanism of deep reinforcement learning is well suited to capturing complex network traffic patterns and improving intrusion detection performance.

Beyond its strong classification results, the proposed model also maintained a low false positive rate, an important requirement for any practical intrusion detection system. Being able to detect multiple attack categories accurately while reducing false alarms highlights the potential of deep reinforcement learning for strengthening network security and supporting more reliable threat detection.

There are several promising directions for future work. The proposed approach could be evaluated on more recent intrusion detection datasets and tested in real-time network environments. More advanced deep reinforcement learning techniques, such as Double DQN and Dueling DQN, could also be explored to further improve detection performance and learning efficiency. Finally, future studies may focus on improving the detection of minority attack categories and integrating the model into live network monitoring and security systems.

REFERENCES

[1] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," IEEE Access, vol. 9, pp. 138432-138450, 2021, doi: 10.1109/ACCESS.2021.3118573.
[2] I. Abrar, Z. Ayub, F. Masoodi and A. M. Bamhdi, "A Machine Learning Approach for Intrusion Detection System on NSL-KDD Dataset," in Proc. Int. Conf. Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 919-924, doi: 10.1109/ICOSEC49089.2020.9215232.
[3] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "Machine Learning and Deep Learning Approaches for CyberSecurity: A Review," IEEE Access, vol. 10, pp. 19572-19585, 2022, doi: 10.1109/ACCESS.2022.3151248.
[4] G. Muhammad, M. S. Hossain and S. Garg, "Stacked Autoencoder-Based Intrusion Detection System to Combat Financial Fraudulent," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2071-2078, 2023, doi: 10.1109/JIOT.2020.3041184.
[5] S. K. Gupta, M. Tripathi and J. Grover, "Hybrid Optimization and Deep Learning Based Intrusion Detection System," Computers and Electrical Engineering, vol. 100, p. 107876, 2022, doi: 10.1016/j.compeleceng.2022.107876.
[6] V. Hnamte and J. Hussain, "DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System," Telematics and Informatics Reports, vol. 10, p. 100053, 2023, doi: 10.1016/j.teler.2023.100053.
[7] S. Seth, K. K. Chahal and G. Singh, "A Novel Ensemble Framework for an Intelligent Intrusion Detection System," IEEE Access, vol. 9, pp. 138451-138467, 2021, doi: 10.1109/ACCESS.2021.3116219.
[8] O. Arreche, I. Bibers and M. Abdallah, "A Two-Level Ensemble Learning Framework for Enhancing Network Intrusion Detection Systems," IEEE Access, vol. 12, pp. 83830-83857, 2024, doi: 10.1109/ACCESS.2024.3407029.
[9] V. Sidharth and C. R. Kavitha, "Network Intrusion Detection System Using Stacking and Boosting Ensemble Methods," in Proc. Third Int. Conf. Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2021, pp. 357-363, doi: 10.1109/ICIRCA51532.2021.9545022.
[10] M. A. Hossain, "Deep Q-Learning Intrusion Detection System (DQ-IDS): A Novel Reinforcement Learning Approach for Adaptive and Self-Learning Cybersecurity," ICT Express, vol. 11, no. 5, pp. 875-880, 2025, doi: 10.1016/j.icte.2025.05.007.
[11] M. Lopez-Martin, B. Carro and A. Sanchez-Esguevillas, "Application of Deep Reinforcement Learning to Intrusion Detection for Supervised Problems," Expert Systems with Applications, vol. 141, p. 112963, 2020, doi: 10.1016/j.eswa.2019.112963.
[12] H. Alavizadeh, H. Alavizadeh and J. Jang-Jaccard, "Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection," Computers, vol. 11, no. 3, p. 41, 2022, doi: 10.3390/computers11030041.
[13] H. Gülmez and P. Angin, "A Study on the Efficacy of Deep Reinforcement Learning for Intrusion Detection," Sakarya University Journal of Computer and Information Sciences, vol. 4, pp. 11-25, 2021, doi: 10.35377/saucis.04.01.834048.
[14] Y. Badr, "Enabling Intrusion Detection Systems with Dueling Double Deep Q-Learning," Digital Transformation and Society, vol. 1, 2022, doi: 10.1108/DTS-05-2022-0016.
[15] Y.-F. Hsu and M. Matsuoka, "A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System," in Proc. IEEE 9th Int. Conf. Cloud Networking (CloudNet), Piscataway, NJ, USA, 2020, pp. 1-6, doi: 10.1109/CloudNet51028.2020.9335796.
[16] M. Tavallaee, E. Bagheri, W. Lu and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in Proc. Second IEEE Symp. Computational Intelligence for Security and Defense Applications (CISDA), 2009.
[17] N. V. Chawla, K. W. Bowyer, L. O. Hall and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321-357, 2002, doi: 10.1613/jair.953.
[18] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, et al., "Human-Level Control Through Deep Reinforcement Learning," Nature, vol. 518, no. 7540, pp. 529-533, 2015, doi: 10.1038/nature14236.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY