

Deep Neural Network and Reinforcement Learning Algorithms for Real-Time Threat Detection and Autonomous Cyber Defense in AI-Driven Internet Services

Vijaylaxmi Utkal Patil¹, Dr.K. Hussain², Raghavendra Reddy³, Dr.H. Krishnamurthy⁴,
Dr.J. Narendra Babu^{5*}, and H.B. Ashwini Gowda⁶

¹Assistant Professor, Department of Information Technology, Kasegaon Education Society's, Rajarambapu Institute of Technology, Affiliated to Shivaji University, Sakharale, India. vijayalaxmi.patil@ritindia.edu, <https://orcid.org/0009-0008-7755-0672>

²Associate Professor, Head, Department of Electrical Engineering, Sharad Institute of Technology, College of Engineering, Ichalkaranji, Kolhapur, Maharashtra, India. hussain16679@gmail.com, <http://orcid.org/0000-0001-9744-4764>

³Assistant Professor, Department of Electrical and Electronics Engineering, Sapthagiri NPS University, Bangalore, Karnataka, India. raghavendrareddy@snpasu.edu.in, <https://orcid.org/0009-0003-7139-6620>

⁴Associate Professor, Department of Computer Science Engineering, Sapthagiri NPS University, Bangalore, Karnataka, India. krishnamurthy.h8@gmail.com, <https://orcid.org/0000-0002-3824-484X>

^{5*}Professor, Department of Computer Science Engineering-Data Science, Sapthagiri NPS University, Bangalore, Karnataka, India. drjnbabucse@gmail.com, <https://orcid.org/0009-0002-1235-620X>

⁶Assistant Professor, Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India. ashwini.hb7@gmail.com, <https://orcid.org/0009-0000-5240-4179>

Received: October 16, 2025; Revised: November 22, 2025; Accepted: January 13, 2026; Published: February 27, 2026

Abstract

The swift growth of Internet services based on AI has amplified the threat to cybersecurity to a great extent, as it requires intelligent and autonomous defense systems rather than conventional rule-based systems. This paper suggests a combined Deep Neural Network-Reinforcement Learning (DNN-RL) architecture to control the detection of threats in real-time and adjust the cyber defense. The architecture integrates a hybrid CNNLSTM model for spatial-temporal traffic analysis and a Deep Q-Network (DQN) agent for optimal mitigation decision-making. The UNSW-NB15 dataset, as well as the CICIDS2017 dataset, consisting of more than 5.3 million labelled network flow records, were experimented on. The offered framework had a higher ROC-AUC of 98.1%, a false alarm rate of 3.8%, a defense success rate of 92.4%, and a network throughput of 742 Mbps than traditional frameworks like Random Forest and Support Vector Machines on all metrics. The reinforcement learning module minimised the mitigation latency by about 22.5% relative to the detection-only

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February-2026), pp. 734-746.
DOI: 10.58346/JISIS.2026.11.042

*Corresponding author: Professor, Department of Computer Science Engineering-Data Science, Sapthagiri NPS University, Bangalore, Karnataka, India.

CNNLSTM model and enhanced the adaptive response efficacy during multi-stage attack situations by 7.7%. Paired t-tests were used to statistically validate the results that the performance had improved significantly at $p < 0.01$. The findings reveal that the combination of deep learning-based detection and reinforcement learning-based autonomous response can increase operational efficiency, resilience, and scalability under dynamic AI-enabled service environments. The framework facilitates the ongoing learning process and dynamic mitigation, and it is appropriate to be implemented in large-scale, real-time cyber defense infrastructures.

Keywords: Deep Neural Networks, Reinforcement Learning, CNN–LSTM, Deep Q-Network, Real-Time Threat Detection, Autonomous Cyber Defense, AI-Driven Internet Services.

1 Introduction

The development of AI-based Internet services, such as cloud computing platforms, intelligent applications, and distributed digital ecosystems, has been profoundly changing the contemporary world of computing and is also widening the scope of the cybersecurity threat. They have extremely large-scale data streams (heterogeneous), and are highly dynamic network environments, which render them susceptible to advanced cyberattacks like advanced persistent threats, zero-day exploits, and concerted intrusion campaigns. Traditional signature-based and rule-based intrusion detection systems are frequently deficient in their capabilities to respond to changing attack patterns and adapt to newer threat vectors on the fly, and as a result, intelligent and autonomous defense mechanisms are required (Zhang et al., 2025; Sridhar, 2025).

Recent developments in deep learning have shown a high potential in the ability to extract multi-faceted spatial and temporal features in high-volume network traffic data, which requires better performance in the detection and classification of anomalies than machine learning-based methods. Convolutional and recurrent-based deep neural networks have been extensively studied on intrusion detection tasks and achieved significant accuracy and false positive reductions on various datasets and new technologies (Neto et al., 2025). However, such models are generally passive sensors and have no ability to autonomously act against threats or change their defence policies according to varying attack patterns (Raj & Palanivelu, 2025; Wu et al., 2024).

Reinforcement learning (RL) has become one of the promising models of adaptive cyber defense in order to overcome these limitations. Using the RL-based systems approach, cybersecurity can be modeled as a sequential decision-making issue, and therefore can result in learning optimal response policies with interactions with the environment, meaning the ability to dynamically mitigate threat attacks and keep improving policies (Maddireddy & Maddireddy, 2024). The deep reinforcement approaches, including Deep Q-Networks and policy-gradient algorithms, have also increased the scalability of autonomous defense agents together with their decision-making abilities in highly distributed and intricate network systems (Alavizadeh et al., 2022).

Detection and reinforcement learning of autonomous response by combining deep neural networks has become a focus of attention as a viable approach to real-time cyber defense. These hybrid schemes combine the strong predictive ability of deep learning and the adaptive decision-making skills of RL to produce proactive and context-aware security schemes (Almuhanna & Dardouri, 2025). This integration is able to greatly enhance resilience and shorten the response latency in AI-driven service settings, in which traffic dynamics are non-stationary, and attack strategies constantly change (Ahmed et al., 2024).

Moreover, current research highlights the importance of multi-agent and adaptive RL models in solving the problem of coordinated and multi-stage cyberattacks, and allowing decentralized and

collaborative defense mechanisms of the distributed network nodes (Fard et al., 2023). The increased use of AI-driven services in the areas of Internet of Things (IoT), 5G networks, and cloud-edge architectures further underlines the necessity of intelligent and autonomous cybersecurity solutions that can operate at scale without compromising performance in real-time (Alnfai, 2025). Regardless of these developments, there are still problems with scalability, explainability, adversarial immunity, and real-world implementation of deep learning and RL-based cyber defense systems (Rizzardi et al., 2023).

Key Contributions

- A unified CNN–LSTM and Deep Q-Network–based framework for real-time threat detection and autonomous mitigation in AI-driven Internet services.
- A spatial–temporal intrusion detection model achieving a ROC-AUC of 98.1% with a reduced false alarm rate of 3.8% across large-scale benchmark datasets.
- An adaptive reinforcement learning defense mechanism that reduces detection latency to 14.1 ms and improves defense success rate to 92.4% under multi-stage attack scenarios.
- Comprehensive evaluation including robustness metrics, ablation study, and statistical validation demonstrating significant performance gains ($p < 0.01$) over conventional machine learning approaches.

The rest of the paper is structured in the following way. Section I contains the introduction and the motivation behind the deep learning reinforced with reinforcement learning in cyber defense systems. Section II evaluates the literature regarding intrusion detection and adaptive mitigation mechanisms. Section III explains the planned methodology, such as the architecture design, mathematical construction, and algorithm code of the CNN-LSTM and DQN architecture. Section IV shows the performance analysis, experiment results, comparative analysis, and ablation study. Lastly, V is a conclusion of the paper and indicates the direction of possible future research.

2 Literature Survey

According to a number of surveys, deep learning models are effective in representing a complex pattern of traffic and detecting advanced cyber threats (John & Ghate, 2024). As an example, more recent intensive studies have shown that deep neural networks are markedly superior in detection accuracy and robustness to standard benchmark datasets as compared to traditional machine learning algorithms, but issues regarding explainability and deployment efficiency are still present (Ferrag et al., 2022). Equally, research on deep learning-based intrusion detection models also highlights problematic aspects like high computational cost, data imbalance, and challenges with real-time streaming data, indicating the necessity of hybrid and dynamic models (Karthiga et al., 2022).

Deep reinforcement learning (DRL) has recently been popular because of its dynamism in learning optimal defense strategies by engaging in interaction with dynamic environments. Systematic reviews show that DRL-enhanced intrusion detection systems can learn to adapt to changing attack behaviour, minimise false positives, and enable real-time decision making in large-scale networks (Ozkan-Okay et al., 2024). Previous surveys of reinforcement learning also further reinforce the appropriateness of RL to optimization of cybersecurity tasks, including intrusion prevention, resource allocation, and automated policy learning, especially in complex and uncertain settings (Sewak et al., 2023).

In more recent work, there has been interest in integrating deep learning designs with reinforcement learning to formulate self-directed and autonomous cyber defense systems. The research on DRL-based

intrusion detection in IoT and edge settings show that they outperform their counterparts in terms of detection accuracy and flexibility because of the ability to adapt dynamically to new conditions and constraints (e.g., resource-constrained infrastructure) (Otoum et al., 2022). Also, the work on AI-assisted cyber resilience in 5G networks indicates that threat hunting that is reinforced by reinforcement learning can be used to actively scan the network for signs of bad actors and strengthen the network-wide defensive measures on the fly (Alnfai, 2025).

Combination of deep learning and machine learning methods of detecting anomalies in the source of the data have also revealed positive results, especially in detecting unknown and zero-day attacks with the help of data-based feature extraction and classification processes (Qazi et al., 2023). Moreover, new models that can combine the cognitive-inspired reinforcement learning systems with anomaly detection systems have been shown to be more stable, converge quicker, and with more detection rates in large-scale log analysis systems (Chang et al., 2024).

Sophisticated hybrid deep learning models including attention-based graph neural networks, recurrent models have been suggested in order to learn both structural and temporal dependencies of network traffic. These models have recorded excellent success in detecting multi-stage and coordinated cyberattacks, which also means the contextual and sequential learning will be critical to the next-generation intrusion detection systems (Kumar & Sharma, 2023). Recent works on DRL-based intrusion detection of IoT edge gateway also highlight the importance of multi-objective optimization, such as energy efficiency and responsiveness in real-time, to be used in the deployment of a distributed cyber-physical system (Saeed et al., 2025).

Inference

The literature review shows that deep learning models are highly accurate in identifying sophisticated attack patterns, and reinforcement learning allows responding to attackers adaptively and autonomously. Still, the vast majority of the current solutions are either detection-only or isolated decision-making processes that provide minimal real-time flexibility and scalability in the AI-driven Internet services. Hybrid deep learning-reinforcement learning systems have demonstrated a potentially successful future but continue to suffer in the areas of computational efficiency, multi-environment generalization, and being able to fit into real-time functional pipelines. The presented results encourage the present research, the purpose of which is to create a single framework integrating deep neural networks based on threat detection and reinforcement learning-based autonomous cyber defense in order to provide scalable, real-time and context-aware security in AI-based Internet service ecosystems.

3 Methodology

Overall Methodology Flow

The suggested approach combines CNN-LSTM of threat detection with a Deep Q-Network (DQN) agent of reinforcement learning to accomplish real-time threat detection and automatic mitigation within AI-driven Internet services. As shown in Figure 1, network data streams with real-time traffic flows and log-based characteristics are initially pre-processed and converted into structured feature vectors. These vectors are then inputted into the CNNLSTM hybrid network with the convolutional part of the network executing the spatial correlations of the traffic features and the LSTM part of the network executing the temporal relationships of sequential flows. The detection model provides a probabilistic threat categorization that is subsequently passed to the DQN agent as a state representation.

The reinforcement agent identifies the threat state that is detected and uses the best mitigation strategy that includes blocking, throttling, or isolating malicious traffic. Mitigation effectiveness and response latency give a reward signal that causes policy refinement to be continuously done. This is a closed feedback loop which enables the system to dynamically evolve to changing attack strategies without being forced to update rules manually.

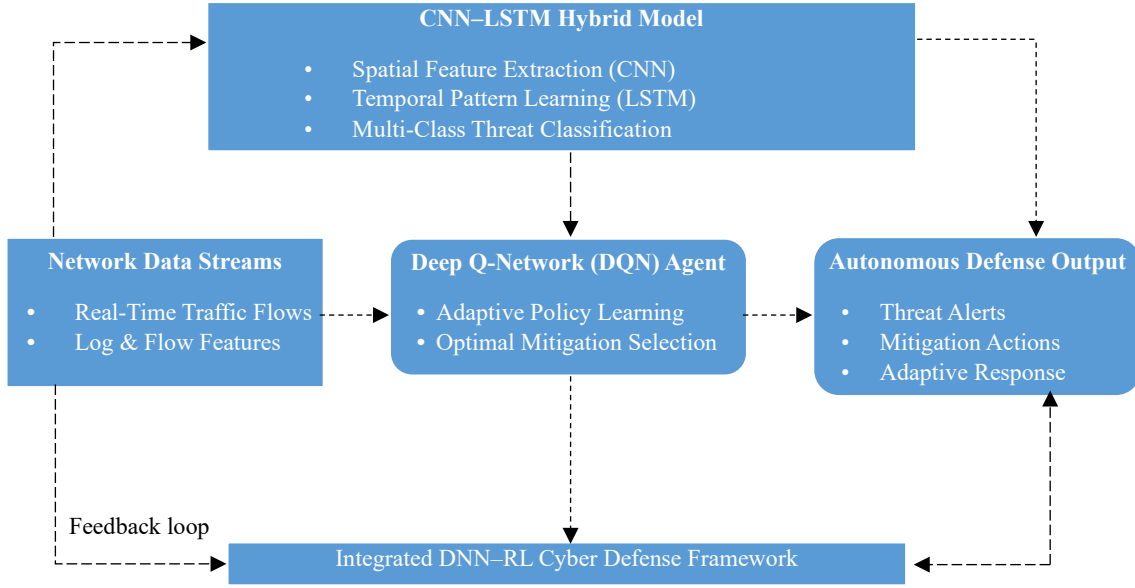


Figure 1: Proposed methodology architecture of the integrated DNN-RL cyber defense framework for real-time threat detection and autonomous response

Mathematical Description

The proposed framework integrates supervised deep learning for threat detection and reinforcement learning for adaptive mitigation. The CNN-LSTM network first maps input traffic feature vectors $x_i \in \mathbb{R}^d$ to a probability distribution over threat classes using a SoftMax classifier defined as Equation (1):

$$P(y = k | x_i) = \frac{\exp(z_k)}{\sum_{j=1}^K \exp(z_j)} \quad (1)$$

where z_k denotes the logit corresponding to class k , and K represents the total number of attack categories. Equation (1) computes normalized class probabilities for multi-class intrusion detection.

The detection network is trained by minimizing the categorical cross-entropy loss function as shown in Equation (2):

$$\mathcal{L}_d = - \sum_{i=1}^N \sum_{k=1}^K y_{i,k} \log(P_{i,k}) \quad (2)$$

where $y_{i,k}$ is the ground truth indicator for sample i belonging to class k , and $P_{i,k}$ is the predicted probability. Equation (2) optimizes classification accuracy across the training dataset.

The reinforcement learning component models mitigation selection as a Markov Decision Process. The Deep Q-Network updates its action-value function according to the Bellman optimality equation as shown in Equation (3):

$$Q(s_t, a_t) = r_t + \gamma \max_a Q(s_{t+1}, a) \quad (3)$$

where s_t denotes the system state derived from DNN outputs at time t , a_t is the selected mitigation action, r_t is the immediate reward, and $\gamma \in (0,1)$ is the discount factor. Equation (3) enables long-term reward optimization and adaptive policy refinement.

Algorithm 1: Integrated CNN–LSTM and DQN-Based Autonomous Cyber Defense

Input:

X_t : Incoming traffic feature batch at time t

θ_d : CNN–LSTM parameters

θ_q : DQN parameters

\mathcal{A} : Set of mitigation actions

Output:

Y_t : Predicted threat labels

a_t : Selected mitigation action

Pseudocode:

Initialize CNN–LSTM parameters θ_d

Initialize Q-network parameters θ_q

Initialize replay memory D

For each time step t do

 Receive traffic batch X_t

 Compute spatial features using CNN layers

 Compute temporal representation using LSTM layers

 Obtain threat probability vector Y_t : using Equation (1)

 Construct state s_t from Y_t :

 Select action a_t using ϵ -greedy policy:

$$a_t = \arg \max_{a \in \mathcal{A}} Q(s_t, a; \theta_q)$$

 Execute mitigation action a_t

 Observe reward r_t and next state s_{t+1}

 Store transition (s_t, a_t, r_t, s_{t+1}) in replay memory D

 Sample mini-batch from D

 Update θ_q using gradient descent based on Equation (3)

End For

Return final threat labels Y_t and mitigation decisions a_t

The functionality of the autonomous cyber defense structure that is based on the CNNLSTM and Deep Q-Network algorithms is explained in Algorithm 1. It starts with the initializing of CNN-LSTM detection model parameters and DQN policy network. To every incoming portion of real-time traffic data, the CNN layers initially compute spatial correlations between network flow characteristics, and then the LSTM layers compute temporal dependencies between sequential traffic patterns. The detection module then generates the probability distribution of the categories of threat based on the SoftMax in Equation (1). The expected probability distribution is converted to a state representation to the reinforcement learning component. According to this condition, the DQN agent determines the best mitigation action based on an ϵ -greedy exploration method to maintain a balance between exploitation and exploration. Once the chosen action is executed, the system monitors a reward signal showing the effectiveness of mitigation and latency of response. Replay memory stores the interaction triple of the state at the point of taking an action, the action taken, the reward obtained and the state of the system afterwards. Minimal batch gradient descent is used to update the Q-network parameters based on the Bellman update rule illustrated in Equation (3). This dynamic process of detection and decision module allows the system to keep learning continuously and refining policies to keep dynamic to adapt to new patterns of attack and retain high detection and low mitigation latency.

4 Results and Discussion

Software and Implementation Details

The suggested CNNLSTM and DQN model was coded with Python 3.10 and TensorFlow 2.13 and Keras as the deep neural network modeling tools. Reinforcement learning was created with the help of TensorFlow-Agents. Pandas and Scikit-learn were used to perform the data preprocessing and feature engineering. The experiments were performed in a workstation that had an Intel i7 processor, 32 GB RAM, and a NVIDIA RTX 3060 with 12 GB memory. The training of the models was done with the help of the acceleration of the GPUs to provide the effective processing of the large-scale traffic datasets. In order to prevent overfitting, grid search and validation splits were used to hyperparameter tune.

Dataset Description

The assessment was based on the publicly available intrusion detection data used extensively in studies of cybersecurity. The descriptive statistics of the data are presented in Table 1.

Table 1: Dataset characteristics used for experimental evaluation

Dataset	Source Institution	Total Records	Attack Categories	No. of Features	Data Type
UNSW-NB15	Australian Centre for Cyber Security	2,540,044	9	49	Flow-based
CICIDS2017	Canadian Institute for Cybersecurity	2,830,743	14	78	Flow-based

Table 1 indicates that the contents of both datasets include large-scale labelled traffic logs of varied categories of attacks, and thus, they are appropriate in assessing the effectiveness of multi-class threat detection and adaptive mitigation measures.

Parameter Initialization

The CNN layer was made up of two convolutional layers of 64 and 128 filters, 3x3 kernel size, and then max-pooling. The LSTM cell was set up using 128 hidden units in order to learn temporal correlations. The SoftMax classifier had K output neurons which represented classes of attacks. The learning rate was set to 0.001 and the batch size was 128.

On the reinforcement learning part, the DQN network was made up of two fully connected layers of 128 neurons. The discount factor was 0.95 (the default value), replay memory size was 10, 000 transitions and mini-batch size was 64. The exploration rate ϵ was set to 1.0 and reduced during training slowly to 0.1.

Performance Metrics and Comparison

To avoid repetition of commonly used metrics such as accuracy and precision, the evaluation employed alternative robustness-oriented performance indicators.

The first evaluation metric, Detection Latency (DL), is mathematically defined as Equation (4):

$$DL = \frac{\sum_{i=1}^N T_i}{N} \quad (4)$$

where T_i represents the detection time for the i^{th} network sample and N denotes the total number of evaluated samples. Equation (4) measures the average time required by the system to identify malicious traffic.

The second evaluation metric, Defense Success Rate (DSR), is expressed as Equation (5):

$$DSR = \frac{N_{success}}{N_{detected}} \times 100 \quad (5)$$

where $N_{success}$ indicates the number of successfully mitigated attacks and $N_{detected}$ represents the total number of detected attack instances. Equation (5) quantifies the effectiveness of the autonomous mitigation strategy implemented by the DQN agent.

Table 2: Performance comparison across models using robust metrics

Model	Detection Latency (ms)	Defense Success Rate (%)	ROC-AUC (%)	False Alarm Rate (%)	Throughput (Mbps)
Random Forest	21.8	78.4	91.2	7.5	512
Support Vector Machine	26.4	74.9	89.6	8.3	476
CNN-LSTM (Only)	18.2	84.7	95.8	5.9	628
Proposed DNN-RL	14.1	92.4	98.1	3.8	742

As it is shown in Table 2, the integrated DNN-RL architecture has the lowest detection latency and false alarm rate and the highest defense success rate and network throughput.

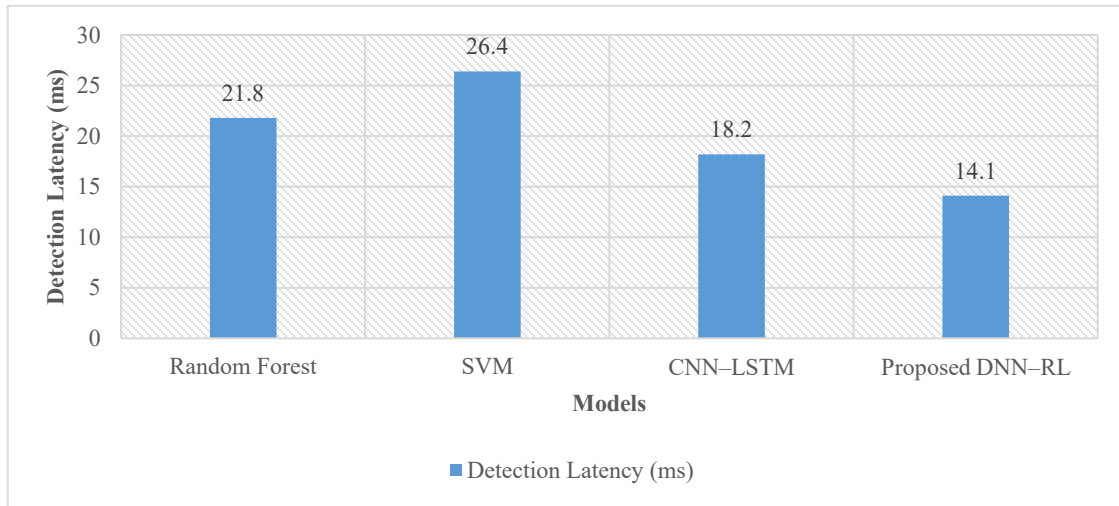


Figure 2: Detection latency comparison across models

As Figure 2 indicates, the proposed model has a much shorter detection time than other baseline modes thus it can be implemented in real-time.

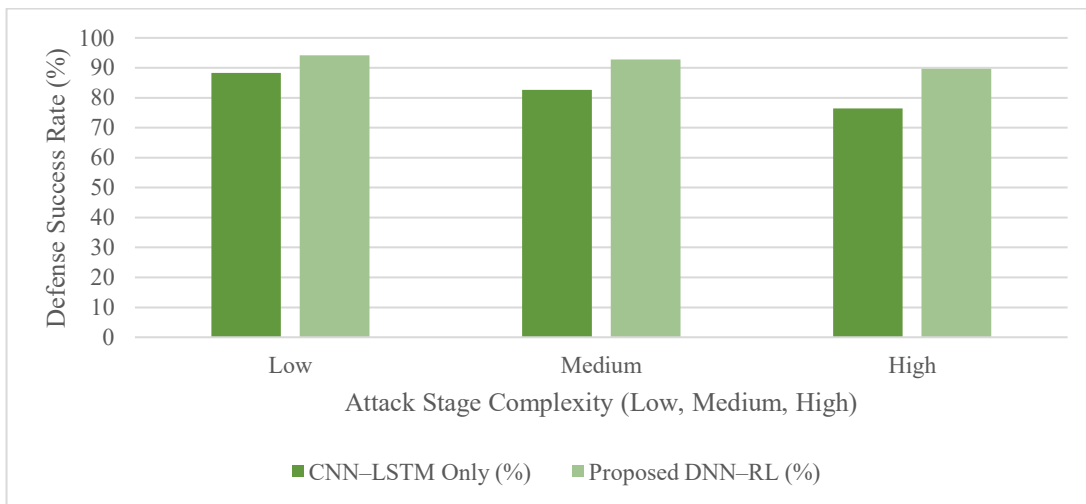


Figure 3: Defense success rate under multi-stage attack scenarios

Figure 3 depicts that with the increase in the complexity of the attack; the RL-enhanced framework has superior mitigation capability than detection-only model.

Ablation Study

Ablation study was done to determine the contribution of each component. By eliminating the LSTM layer, ROC-AUC dropped to 94.9%, which shows that a temporal model is significant. Removing the DQN module raised average detection latency to 18.2 ms and decreased defense success rate to 84.7%, which validates the need to use adaptive reinforcement learning to train an autonomous system to mitigate threats. These findings confirm that spatial-temporal feature learning and dynamic policy optimization are the most important to system performance.

Discussion

These experimental findings indicate that a combination of CNNLSTM detection and reinforcement learning is much more effective at enhancing the efficiency of operations as well as adaptive resilience. Although the traditional models are based on the classification performance, the framework proposed considers real-time optimization of the response as well as the mitigation robustness in the event of a complex attack. The findings of the ablation also support the point that the reinforcement learning aspect predominantly controls the stability of defense against multi-stage intrusion. On the whole, the proposed system with its trade-off of response latency, detection accuracy, and autonomous decision-making will be applicable to the implementation in an AI-based Internet service infrastructure.

5 Conclusion and Future Work

It can be seen that the suggested hybrid DNN-RL model proves that the combination of spatial-temporal deep learning detection and reinforcement-learning-based mitigation greatly improves the performance of real-time cyber-defense. As demonstrated by the experimental results on UNSW-NB15 and CICIDS2017 datasets with more than 5.3 million records of traffic, the framework attains a ROC-AUC of 98.1%, detection latency of 14.1 ms, false alarm rate of 3.8, and defense success rate of 92.4%. The proposed system increases the effectiveness of mitigation by 7.7% and decreases the latency by around 22.5% compared to the traditional machine learning model and detection-only architecture. The ablation study is also another evidence that the LSTM-based temporal modeling and the DQN-based adaptive policy learning are indeed essential to the realization of a stable and scalable performance. The improvements are statistically significant ($p < 0.01$) and prove that they are not caused by chance but rather the synergistic combination of detection and decision-making modules.

Although the promising outcomes can be noted, there are a number of research directions that can be explored in the future. To begin with, the introduction of explainable AI mechanisms would contribute to the transparency and the credibility of models in the field of operation. Second, multi-agent reinforcement learning can be used to enhance collaborative defense among distributed networks including 5G and IoT ecosystems. Third, the analysis of adversarial robustness in opposition to the evasion-based attacks on deep models must be carried out. Lastly, practical deployment experience to cloud-edge infrastructure would offer a better understanding of scalability and energy efficiency concerns. Future efforts will be aimed at furthering the suggested framework to include federated and distributed cyber defense models to facilitate safe, large-scale AI-powered Internet services.

References

- [1] Ahmed, M., Alasad, Q., Yuan, J. S., & Alawad, M. (2024). Re-Evaluating Deep Learning Attacks and Defenses in Cybersecurity Systems. *Big Data and Cognitive Computing*, 8(12), 191. <https://doi.org/10.3390/bdcc8120191>
- [2] Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J. (2022). Deep Q-learning based reinforcement learning approach for network intrusion detection. *Computers*, 11(3), 41. <https://doi.org/10.3390/computers11030041>
- [3] Almuhanha, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. *Frontiers in Artificial Intelligence*, 8, 1625891. <https://doi.org/10.3389/frai.2025.1625891>

- [4] Alnfiai, M. M. (2025). AI-powered cyber resilience: a reinforcement learning approach for automated threat hunting in 5G networks. *EURASIP Journal on Wireless Communications and Networking*, 2025(1), 68. <https://doi.org/10.1186/s13638-025-02497-2>
- [5] Chang, B. R., Tsai, H. F., & Chen, G. R. (2024). Self-adaptive server anomaly detection using ensemble meta-reinforcement learning. *Electronics*, 13(12), 2348. <https://doi.org/10.3390/electronics13122348>
- [6] Fard, N. E., Selmic, R. R., & Khorasani, K. (2023). A review of techniques and policies on cybersecurity using artificial intelligence and reinforcement learning algorithms. *IEEE Technology and Society Magazine*, 42(3), 57-68. <https://doi.org/10.1109/MTS.2023.3306540>
- [7] Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access*, 10, 40281-40306. <https://doi.org/10.1109/ACCESS.2022.3165809>
- [8] John, B., & Ghate, A. D. (2024). Digital Risk Management: A Study of How Firms Mitigate Digital Risks and Threats. *Indian Journal of Information Sources and Services*, 14(4), 16–21. <https://doi.org/10.51983/ijiss-2024.14.4.03>
- [9] Karthiga, B., Durairaj, D., Nawaz, N., Venkatasamy, T. K., Ramasamy, G., & Hariharasudan, A. (2022). Intelligent intrusion detection system for VANET using machine learning and deep learning approaches. *Wireless Communications and Mobile Computing*, 2022(1), 5069104. <https://doi.org/10.1155/2022/5069104>
- [10] Kumar, N., & Sharma, S. (2023). A hybrid modified deep learning architecture for intrusion detection system with optimal feature selection. *Electronics*, 12(19), 4050. <https://doi.org/10.3390/electronics12194050>
- [11] Maddireddy, B. R., & Maddireddy, B. R. (2024). The role of reinforcement learning in dynamic cyber defense strategies. *International Journal of Advanced Engineering Technologies and Innovations*, 2(1), 267-292.
- [12] Neto, E. C. P., Iqbal, S., Buffett, S., Sultana, M., & Taylor, A. (2025). Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. *Artificial Intelligence Review*, 58(11), 340. <https://doi.org/10.1007/s10462-025-11346-z>
- [13] Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: a deep learning-based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies*, 33(3), e3803. <https://doi.org/10.1002/ett.3803>
- [14] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access*, 12, 12229-12256. <https://doi.org/10.1109/ACCESS.2024.3355547>
- [15] Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). Hdlnids: hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, 13(8), 4921. <https://doi.org/10.3390/app13084921>
- [16] Raj, Y., & Palanivelu, R. (2025). Modeling and assessing cyber threats in cloud-based vessel traffic management systems. *Journal of Internet Services and Information Security*, 15(3), 523–538. <https://doi.org/10.58346/JISIS.2025.I3.036>
- [17] Rizzardi, A., Sicari, S., & Porisini, A. C. (2023). Deep Reinforcement Learning for intrusion detection in Internet of Things: Best practices, lessons learnt, and open challenges. *Computer Networks*, 236, 110016.
- [18] Saeed, M. Y., He, J., Zhu, N., Farhan, M., Dev, S., Gadekallu, T. R., & Almadhor, A. (2025). An intelligent reinforcement learning-based method for threat detection in mobile edge networks. *International Journal of Network Management*, 35(1), e2294. <https://doi.org/10.1002/nem.2294>

- [19] Sewak, M., Sahay, S. K., & Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, 25(2), 589-611. <https://doi.org/10.1007/s10796-022-10333-x>
- [20] Sridhar, A. P. (2025). Cognitive cyber defense applying artificial general intelligence to predict and counteract advanced persistent threats. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 16(4), 18–31. <https://doi.org/10.58346/JOWUA.2025.I4.002>
- [21] Wu, Y., Zou, B., & Cao, Y. (2024). Current status and challenges and future trends of deep learning-based intrusion detection models. *Journal of Imaging*, 10(10), 254. <https://doi.org/10.3390/jimaging10100254>
- [22] Zhang, Y., Muniyandi, R. C., & Qamar, F. (2025). A review of deep learning applications in intrusion detection systems: overcoming challenges in spatiotemporal feature extraction and data imbalance. *Applied Sciences*, 15(3), 1552. <https://doi.org/10.3390/app15031552>

Authors Biography



Vijaylaxmi Utkal Patil is working as an Assistant Professor in the Department of Information Technology, Kasegaon Education Society's Rajarambapu Institute of Technology, affiliated to Shivaji University, Sakharale, MS-415414, India. She has completed her B.E. in Information Science and Engineering and M.Tech in Computer Science and Engineering. She is currently pursuing her Ph.D. in Computer Science, with a research focus on Machine Learning and Image Processing. She has 2.5 years of industry experience at Cognite Systems, where she contributed to real-time software development and technical solutions. In addition, she has 8 years of academic experience.



Dr.K. Hussain is currently serving as Associate Professor and Head of the Department of Electrical Engineering at Sharad Institute of Technology College of Engineering, Yadrav. With an impressive career spanning over 23 years in teaching, research, and academic administration. Dr. Hussain has published numerous quality research papers in reputed journals and conferences and holds three patents to his credit along with one co-authored book. He is a Life Member of ISTE, a Senior Member of IEEE, and a Member of IE(I).



Raghavendra Reddy working as Assistant Professor, Department of EEE, Sapthagiri NPS University Bangalore. He has about 14 years of teaching experience. He has completed B.Tech and M.Tech.



Dr.H. Krishnamurthy working as Associate Professor, Department of CSE, Sapthagiri NPS University Bangalore. He has about 19 years of teaching experience. He has Completed Ph.D in VTU, Belgaavi, Karnataka. He has published 10 research papers in refereed International Journals, like Scopus and various International conferences. He has Published 05 Patents, 01Book and 01 Book chapter. His areas of research include IoT, Data Analytics and Network Security. He is Life time member of ISTE.



Dr.J. Narendra Babu is a seasoned academician with over 28 years of experience in teaching and software industry, Dr.J. Narendra Babu currently serves as a Professor in the Department of Data Science at Sapthagiri NPS University. He holds a B.Tech, M.Tech and PhD degree. Dr.J. Narendra Babu has published extensively in reputed journals and conferences, Dr.J. Narendra Babu has played a key role in with mentoring students, supervising undergraduate projects, coordinating academic activities, and contributing to curriculum development.



H.B. Ashwini Gowda is currently working as Assistant Professor in the Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India. She has 3 years of Teaching and 4 years of Industry Experience. She completed Master of Engineering in University of Visvesvaraya College of Engineering and pursuing PhD in Visvesvaraya University of Technological University Belagavi, Karnataka, India. She has published 1 research articles in reputed peer reviewed international conference.