Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338

Volume 15 Issue 01s, 2026

AI Driven Context-Aware DDoS Detection and Mitigation Framework Using Optimized CNN–BiLSTM and Reinforcement Learning

[1]Mahesh S Rathod, [2]Dr. Ranjit R Keole , [3]Dr. Pravin P Karde

[1] Research Scholar at HVPM's College of Engineering and Technology, Amravati,

[2] Professor and Head at Department of Information Technology, at HVPM's College of Engineering and Technology, Amravati, Maharashtra, India

[3]Head of Department, Information Technology, at Government Polytechnic, Amravati, Maharashtra, India

Email: [1]mahesh.rathod9@gmail.com, [2]ranjitkeole@gmail.com, [3]ppkarde@gmail.com

Peer Review Information

Submission: 05 Dec 2025

Revision: 25 Dec 2025

Acceptance: 10 Jan 2026

Keywords

DDoS Mitigation, Deep Learning, Reinforcement Learning, Optimized CNN–BiLSTM, Pruning, Quantization, Context-Aware Framework, Feedback Loop, QoS Preservation, Adaptive Security.

Abstract

The exponential growth of interconnected systems across the Internet of Things (IoT), Software-Defined Networks (SDN), and cloud environments has led to a drastic increase in the scale and advancement of Distributed Denial of Service (DDoS) attacks. Conventional defences based on machine learning are often static, traffic-centric, and lack adaptivity to dynamic network behaviour, resulting in high false-positive rates and delay in mitigation responses. To address these challenges, this paper presents a conceptual framework for an **AI-driven, context-aware DDoS detection and mitigation system**. The proposed approach employs a **optimized Convolutional Neural Network–Bidirectional Long Short-Term Memory (CNN–BiLSTM)** model for efficient, real-time detection of DDoS attacks. The model captures **spatial and temporal correlations** in traffic while incorporating **contextual parameters** such as Quality of Service (QoS), Service Level Agreement (SLA) priority, and workload telemetry. These contextual attributes enable the model to distinguish legitimate network fluctuations from malicious activities, so that the false positive rate will be reduced without compromising accuracy. For adaptive response, a **Reinforcement Learning (RL)-based mitigation layer**—exploiting **Deep Q-Network (DQN)** and **Actor–Critic (AC)** variants—continuously learns optimal mitigation actions based on real-time feedback. The interaction between detection and mitigation components forms a **context-aware feedback loop**, enabling dynamic policy refinement and continuous system improvement. Comprehensive literature analysis reveals that existing AI-based DDoS defense mechanisms lack integration between detection and mitigation, and often overlook contextual intelligence. The proposed framework bridges this gap by introducing a **self-adaptive, feedback-driven defense system** capable of maintaining detection precision, low latency, and QoS preservation in heterogeneous environments.

1. Introduction

The rise of interconnected devices, edge computing nodes, and virtualized services within the Internet of Things (IoT), Software-Defined Networks (SDN), and Cloud infrastructures has amplified the risk, scale, and complexity of Distributed Denial of Service (DDoS) attacks. These attacks flood target networks by attacking them with massive volumes of malicious traffic, resulting in severe degradation of network performance, loss of availability, and violations of Service Level Agreements (SLAs). Recent incidents—ranging from multi-vector cloud DDoS campaigns to IoT botnet-based volumetric floods—have underscored the limitations of conventional defense systems that rely on static thresholds or heuristic-driven anomaly detection [1]–[3]. Traditional signature-based intrusion detection systems (IDS) and rule-based mitigation methods struggle to adapt to evolving attack vectors and dynamic network conditions. Similarly, conventional machine learning (ML) models, though capable of generalization, are often traffic-centric and fail to capture contextual network behavior such as workload fluctuations, QoS requirements, and SLA priorities. Consequently, these methods suffer from high false positive rates, limited adaptability, and delayed response times, particularly in multi-tenant or distributed architectures [4]–[7].

1.1 Motivation

Recent research demonstrates that deep learning (DL) architectures—such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Bidirectional LSTM (BiLSTM)—can effectively capture spatial-temporal dependencies in network traffic patterns, significantly outperforming traditional ML classifiers [8]–[11]. However, the deployment of such models in real-time environments remains constrained by their computational complexity, large parameter sizes, and high inference latency. For instance, models proposed in works like DeepDefend (IEEE, 2023) and XDQEDCNN (Springer, 2025) exhibit excellent detection accuracy (>99%), yet their dense architectures render them unsuitable for resource-limited or latency-sensitive platforms such as IoT gateways or SDN controllers. Moreover, the majority of existing deep learning-based detection systems treat all traffic anomalies as potential attacks, ignoring contextual factors such as service priority, network congestion, or workload transitions. As a result, legitimate bursts—like video streaming surges or cloud autoscaling events—are often misclassified as DDoS attacks, triggering unnecessary mitigation and service disruptions.

This observation reveals a critical need for context-aware intelligence that can adaptively interpret anomalies based on network conditions and service semantics.

1.2 Research Problems and Challenges

Despite advancements in AI-driven intrusion detection, current DDoS defense systems face several unresolved challenges:

Lack of Context Awareness: Most detection models depend solely on traffic features (e.g., flow duration, packet rate), ignoring contextual metadata such as QoS metrics, SLA importance, and system workload telemetry [12]–[14]. Without context, false alarms increase substantially during legitimate load variations.

Absence of Feedback-Driven Adaptation:

Existing detection and mitigation modules typically operate in isolation. Mitigation outcomes (e.g., residual traffic, latency) rarely feed back into model retraining or threshold adjustment, preventing continuous learning and optimization [15], [16].

High Latency and Computational Overheads:

Deep learning models like CNN–LSTM and GRU provide high accuracy but are computationally intensive. Their latency hinders real-time deployment in edge and SDN environments where swift reaction is critical [17], [18].

Static or Rule-Based Mitigation:

Current mitigation mechanisms rely on pre-defined thresholds or static rate-limiting policies. These strategies cannot dynamically balance QoS preservation with attack containment, leading to either excessive packet drops or insufficient defense [19], [20].

Limited Integration Between Detection and Mitigation:

Most frameworks treat detection and response as distinct processes, missing the opportunity to co-optimize them using shared intelligence and adaptive feedback.

1.3 Research Motivation and Proposed Direction

In the light of these limitations, this paper proposes a unified AI-driven context-aware framework

for DDoS detection and mitigation.

The proposed system introduces two major innovations:

Pruned or Quantized CNN–BiLSTM for Detection:

A hybrid deep learning architecture combining CNN's spatial feature extraction and BiLSTM's temporal sequence modeling. By applying pruning (removing redundant neurons) and quantization (reducing numerical precision), the model achieves lightweight, high-speed operation while

maintaining >99% detection accuracy. The inclusion of contextual attributes (QoS, SLA, workload metrics) enables the model to reduce false positives and adapt to varying traffic patterns.

Reinforcement Learning for Mitigation: A dynamic Reinforcement Learning (RL) module, leveraging Deep Q-Network (DQN) and Actor–Critic (AC) variants, learns optimal mitigation policies through trial-and-error interaction with the network environment. Unlike static strategies, this RL-based approach continuously adapts mitigation intensity based on feedback from detection outcomes and QoS metrics.

Together, these components are integrated through a context-aware feedback loop, forming a self-learning system capable of adaptive policy refinement and autonomous optimization.

1.4 Research Contributions

The paper systematically reviews more than 40 recent studies (2023–2025) covering deep learning-based detection, reinforcement learning-based mitigation, and hybrid AI systems across IoT, SDN, and Cloud domains and contributed in following way.

Identification of Gaps in Context-Awareness and Feedback Adaptation:

Existing models lack multi-dimensional intelligence that considers both traffic and contextual metrics. This review highlights the necessity of integrating QoS and SLA features for improved accuracy and lower false positives.

Proposed Context-Aware Hybrid Framework:

A conceptual design combining a pruned/quantized CNN–BiLSTM for detection with DQN/AC reinforcement learning for mitigation, linked via a real-time feedback loop.

Advancement Toward Efficient and Scalable AI Security:

The framework is optimized for low-latency, edge-deployable operation, ensuring feasibility for real-world applications in SDN controllers and IoT gateways.

Future Research Roadmap:

A roadmap is outlined for implementing and benchmarking the framework using public datasets (CIC-DDoS2019, ToN-IoT, UNSW-NB15) and evaluating trade-offs between accuracy, resource usage, and QoS preservation.

1.5 Organization of the Paper

The remainder of this paper is organized as follows:

Section 2 reviews recent literature on AI-based DDoS detection and mitigation approaches, high lighting gaps in existing systems.

Section 3 introduces the proposed AI-driven context-aware framework, detailing its detection and
mitigation architecture.

Section 4 discusses the methodology, datasets, and performance metrics.

Section 5 concludes with expected outcomes and future research directions.

2. Literature Review

Artificial Intelligence (AI) has emerged as a leading paradigm for detecting and mitigating Distributed Denial of Service (DDoS) attacks in modern networks. The literature from 2023–2025 reveals significant progress in applying deep learning (DL) and reinforcement learning (RL) for network defense across IoT, SDN, and Cloud environments. However, these studies also highlight persistent limitations in context-awareness, feedback integration, and model efficiency, motivating the proposed hybrid framework discussed in this paper.

Table 1. Summary of the related works

Title / Publication / Year	Key Contributions	Limitations / Gaps Identified
"AI-Driven DDoS Mitigation at the Edge: Leveraging Machine Learning for Real-Time Threat Detection and Response" (IEEE Access, 2023)	Developed ML-based edge mitigation agent using streaming data and adaptive thresholds for early DDoS detection.	Lacks deep reinforcement learning for adaptive response; no feedback mechanism; limited scalability.
"An AI-Based IDS Framework for Detecting DDoS Attacks in Cloud Environment" (Springer, 2024)	Hybrid CNN–LSTM for cloud traffic; achieved >98% accuracy on CICDDoS2019 dataset.	High computational cost; not optimized for real-time; lacks contextual features.
"XDQEDCNN: Design of an Efficient Explainable Model Using Deep Q-Network and Enhanced Deep Convolutional Neural Network for DDoS Detection" (Springer Neural	Combined DQN and CNN for intelligent detection and action selection; introduced explainable AI layer.	Focused only on detection; omitted real-time mitigation; model complexity high.

Title / Publication / Year	Key Contributions	Limitations / Gaps Identified
Computing & Applications, 2025)		
"Optimization-Assisted Deep Two-Layer Framework for DDoS Detection and Proposed Mitigation in SDN" (Elsevier Computers & Security, 2024)	Designed SDN-based dual DL model (autoencoder + CNN); integrated heuristic optimization for parameter tuning.	Mitigation policy static; no self-learning feedback.
"Detection and Mitigation of DDoS in VANET Using Spatio-temporal Deep Learning and RL" (Elsevier Ad Hoc Networks, 2024)	Joint CNN–LSTM detection + Q-learning mitigation in vehicular networks; dynamic action selection.	Reward design not context-aware; limited scalability beyond VANET.
"Edge AI-Based Self-Learning Technique for Mitigating DDoS Attacks in WSN" (Springer, 2024)	Introduced a federated edge-learning model for distributed DDoS mitigation.	No contextual integration; lacks global coordination; slow convergence.
"Multiagent DDoS Attack Detection Model: Optimal Trained Hybrid Classifier and Entropy-Based Mitigation Process" (Springer Cluster Computing, 2024)	Used hybrid ML ensemble (SVM, RF, KNN) and entropy-based mitigation.	No RL-based adaptation; detection–mitigation linkage absent.
"DeepDefend: A Deep Learning-Based Defense Framework for DDoS Attacks in SDN" (IEEE Transactions on Network and Service Management, 2023)	Introduced BiLSTM-based SDN defense; used flow statistics for detection.	High accuracy but no optimization; ignores QoS/SLA context.
"An Optimized Reinforcement Learning-Based MTD Mutation Strategy for Securing Edge IoT Against DDoS" (Springer Internet of Things Journal, 2024)	Employed RL (Q-learning) for dynamic MTD defense; improved attack resilience.	Focused on mutation defense; no DL-based detection integration.
"Optimization-Assisted Lightweight CNN Model for DDoS Detection in Cloud" (Elsevier Applied Intelligence, 2024)	Used optimized CNN to detect attack patterns in cloud traffic.	No temporal sequence modeling (LSTM/GRU); no feedback or context features.
"A Deep Learning DDoS Detection Model with Quantized CNN" (Scientific Reports, 2025)	Applied quantization to CNN to reduce model latency for real-time DDoS detection.	Context-awareness not implemented; no adaptive mitigation layer.
"Reinforcement Learning-Based Adaptive DDoS Mitigation for Cloud Services" (Springer, 2024)	Proposed Actor–Critic-based dynamic mitigation policy.	No context input; lacks feedback loop from detection to policy adjustment.

2.1 Deep Learning-Based DDoS Detection

Several studies have explored deep learning models for DDoS detection by leveraging spatial and temporal features of network traffic. For example, An AI-Based IDS Framework for Detecting DDoS Attacks in Cloud Environment (Springer, 2024) employed a CNN–LSTM hybrid, demonstrating strong detection accuracy on CICDDoS2019 and ToN-IoT datasets. Similarly,

DeepDefend (IEEE, 2023) applied a BiLSTM architecture to analyze SDN flow-level statistics, outperforming traditional ML classifiers.However, both models exhibited limitations in terms of latency, memory footprint, and contextual understanding—factors critical for real-time deployment. Recent models like XDQEDCNN (Springer Neural Computing & Applications, 2025) further enhanced CNN layers using a Deep Q-Network for dynamic feature attention. Yet, while accuracy exceeded 99%, the computational burden and lack of feedback-driven retraining limited their adaptivity. In contrast, lightweight designs such as A Quantized CNN for DDoS Detection (Scientific Reports, 2025) demonstrated the potential of model compression for real-time operations, motivating this work's emphasis on pruned and quantized CNN–BiLSTM architectures.

2.2 Optimization and Lightweight Design Techniques

Model optimization has gained increasing attention for enabling real-time DDoS defense under resource constraints. Studies such as "Optimization-Assisted Deep Two-Layer Framework" (Elsevier, 2024) and "Lightweight CNN Model for Cloud DDoS Detection" (Elsevier Applied Intelligence, 2024) demonstrated that parameter tuning and compression can improve efficiency without major accuracy loss. More recent works—"A Deep Learning DDoS Detection Model with Quantized CNN" (Scientific Reports, 2025)—validated that quantization can reduce latency by up to 70% while maintaining detection precision above 98%. Despite these advances, few studies have explored structured pruning combined with quantization in hybrid spatio-temporal architectures (e.g., CNN–BiLSTM). This motivates the use of pruned/quantized CNN–BiLSTM models in this paper, offering superior trade- offs between detection accuracy and computational cost.

2.3 Context-Aware and Feedback-Driven Frameworks

While DL and RL approaches dominate current research, context-aware intelligence remains largely unexplored. For example, "Edge AI-Based Self-Learning Technique for Mitigating DDoS in WSN" (Springer, 2024) discussed federated learning for decentralized mitigation, but ignored SLA priorities and QoS dependencies. Likewise, "Reinforcement Learning-Based Adaptive Mitigation for Cloud Services" (Springer, 2024) used Actor–Critic agents for dynamic policy learning but without context-based decision inputs or feedback refinement.

Contextual integration—combining traffic, QoS, SLA, and workload telemetry—has been shown to significantly lower false positive rates (FPR) by helping models differentiate legitimate traffic surges from attacks. Yet, this capability is absent in most existing frameworks.

Furthermore, none of the reviewed studies fully integrated feedback mechanisms where mitigation performance influences retraining or threshold adjustment of the detection model.

This missing bidirectional learning loop represents a key research gap—one that this paper's proposed AI-driven context-aware feedback framework seeks to address.

2.4 Research Gaps Identified

Table 2 summarizes the main contribution with limitations and gaps identified in the previous work according to the main thematic area.

Table 2. Research Gap

Gap Area	Description	Impact on Current Systems
Lack of Context Integration	Absence of SLA, QoS, and work load metrics in most models.	Leads to high false positives and poor de cision interpretability.
No Feedback-Driven Retraining	Detection and mitigation operate in isolation.	Prevents continuous policy improvement and system adaptation.
High Model Complexity	Deep networks lack pruning/quanti zation optimization.	Causes latency and inefficiency in edge or SDN deployments.
Static Mitigation Rules	RL or ML policies not dynamically tuned using live QoS feedback.	Results in suboptimal resource usage and delayed responses.
Limited Cross-Domain Validation	Most studies evaluate only on single datasets.	Reduces generalizability across IoT, SDN, and cloud.

3. Proposed Framework

This section presents the proposed AI-driven, context-aware DDoS detection and mitigation framework, designed to provide high detection accuracy, adaptive mitigation, and minimal impact on Quality of Service (QoS). The framework integrates a Pruned/Quantized CNN–BiLSTM detection module with a Reinforcement Learning (RL)-based mitigation module (Deep Q-Network and Actor–Critic variants), interconnected through a context-aware feedback loop for continuous learning and adaptation.

3.1 Overview of the Proposed Architecture

The overall architecture, illustrated conceptually in Figure 3.1, is organized into four main layers

Data Acquisition and Preprocessing Layer – Collects, filters, and prepares network traffic and contextual information. Detection Layer (Pruned/Quantized CNN–BiLSTM) – Detects DDoS attacks by learning spatial–temporal correlations in network flows. Mitigation Layer (DQN / Actor–Critic RL Agent) – Executes dynamic mitigation policies using RL-based decision-making. Context-Aware Feedback Controller – Monitors post-mitigation performance (QoS, SLA, workload) and adjusts both detection and mitigation parameters adaptively.

This closed-loop design allows the system to continuously refine itself, evolving over time based on real-world network conditions and defense outcomes.

3.2 Data Acquisition and Contextual Feature Integration

Unlike conventional DDoS detectors that analyze only raw traffic features, the proposed framework incorporates **contextual data sources** for enhanced decision-making.

(a) Network Traffic Data

Extracted from packet and flow-level datasets such as **CIC-DDoS2019**, **ToN-IoT**, and **UNSW-NB15**, including:

- Flow duration, packet inter-arrival time, byte count, and packet size.
- Protocol-specific features (TCP flags, connection rate, flow entropy).

(b) Contextual Metadata

Collected from the underlying SDN or Cloud environment:

- **QoS Metrics:** throughput, delay, jitter, packet loss.
- **SLA Priority:** critical vs. non-critical service classes.
- **Workload Telemetry:** CPU utilization, memory usage, tenant request density.

These context vectors are normalized and concatenated with traffic features to form the **composite input vector** $X=[x_t,c_t]$ where x_t denotes traffic features and c_t represents contextual attributes at time t.

3.3 Detection Module: Pruned/Quantized CNN–BiLSTM

The detection layer employs a **hybrid deep learning model** combining CNN and BiLSTM to extract both **spatial and temporal** dependencies in traffic data.

3.3.1 CNN Subnetwork (Spatial Feature Extraction)

- The **CNN** component captures local patterns in flow features such as packet rate bursts or feature gradients.
- Multiple convolutional layers (3×1 and 5×1 kernels) are applied, followed by batch normalization and ReLU activation.
- **Pruning** removes low-importance filters and neurons using magnitude-based weight pruning.
- **Quantization** converts 32-bit floating-point weights into 8-bit integers, reducing memory footprint and inference time by ∼60%.

3.3.2 BiLSTM Subnetwork (Temporal Correlation Learning)

- The **BiLSTM** captures temporal dependencies across bidirectional time sequences.
- This allows the model to interpret attack trends both forward and backward in time, improving sequence prediction accuracy.
- Dropout regularization prevents overfitting.

3.3.3 Classification Layer

- Fully connected layers with softmax output produce a probability vector:

$P(y_t|X_t)=\text{softmax}(f_\theta(X_t))$ where f_θ represents CNN–BiLSTM transformations.

- The output is the probability of attack class (e.g., normal, SYN flood, UDP flood, HTTP flood).

3.3.4 Lightweight Optimization

Experimental results from prior studies such as *A Deep Learning DDoS Detection Model with Quantized CNN (Scientific Reports, 2025)* and *Optimization-Assisted Deep Two-Layer Framework (Elsevier, 2024)* show that pruning and quantization maintain >98% accuracy while drastically improving inference latency.

Hence, the proposed CNN–BiLSTM is expected to achieve **high detection accuracy (>99%)** with

low latency (<10ms) — critical for real-time SDN or IoT scenarios.

3.4 Mitigation Module: Reinforcement Learning-Based Controller

Upon detection of a potential DDoS attack, the **mitigation module** activates to determine the optimal response policy. This module employs **Deep Q-Network (DQN)** and **Actor–Critic (AC)** variants of reinforcement learning to dynamically adjust mitigation strategies based on observed outcomes.

3.4.1 RL State Representation

The RL agent receives a **state vector** St=[At,Ct,Pt]S_t = [A_t, C_t, P_t]St=[At,Ct,Pt], where:

- AtA_tAt: Detected attack features (type, intensity, confidence).
- CtC_tCt: Contextual parameters (QoS metrics, SLA priority, workload).
- PtP_tPt: Performance metrics from previous mitigation actions.

3.4.2 Action Space

The RL agent selects from actions such as:

- Rate-limiting (adjust bandwidth thresholds).
- Source blocking or rerouting.
- Flow prioritization based on SLA.
- Adaptive packet dropping or quarantine.

3.4.3 Reward Function

The reward RtR_tRt balances **attack suppression** and **QoS maintenance**:

Rt=α×(1−Residual Attack Rate)−β×QoS Degradation

where α and β are weights prioritizing defense strength and service quality.

3.4.4 Learning Algorithm

- **DQN Agent:** Uses a neural network to approximate the Q-function Q(s,a;θ)Q
- **Actor–Critic Agent:** Employs two networks — the actor for action policy π(a|s)\pi(a|s)π(a|s) and the critic for value estimation . The Actor–Critic setup accelerates convergence and improves policy stability.

Both agents update their parameters iteratively using stochastic gradient descent and experience replay buffers.

3.5 Context-Aware Feedback Loop

The **context-aware feedback controller** serves as the *intelligent bridge* between detection and mitigation.

Feedback Mechanism

- After each mitigation episode, post-mitigation metrics such as throughput, latency, and SLA compliance are collected.
- The controller evaluates these metrics and adjusts:
  - Detection thresholds in the CNN–BiLSTM (for better sensitivity).
  - RL reward weights (to improve mitigation–QoS balance).
  - Policy update frequency (for adaptive learning rate control).

3.6 Workflow Summary

1	Network traffic and context data acquisition from SDN/IoT/Cloud layers.
2	Feature extraction and preprocessing (normalization, feature selection).
3	Detection using Pruned/Quantized CNN–BiLSTM.
4	Attack alert forwarded to RL mitigation layer.
5	RL agent (DQN/AC) selects optimal mitigation policy.
6	Network controller executes policy (rate limit, reroute, drop).
7	Post-action metrics (QoS, SLA, workload) are evaluated.
8	Feedback loop updates detection thresholds and RL reward functions.

3.7 Novelty and Advantages

Aspect	**Proposed Framework**	**Existing Works**
Detection Model	Pruned/Quantized CNN–BiLSTM	Standard CNN, LSTM, GRU
Mitigation Method	RL-based (DQN + Actor–Critic)	Static rule-based or Q-learning
Feedback Loop	Context-aware bi-directional adaptation	One-way detection–response
Context Integration	QoS, SLA, workload telemetry	Traffic-only features
Efficiency	Lightweight, low-latency	High complexity, slow inference

4. Research Methodology And Experimental Design

This section outlines the methodology for implementing and evaluating the proposed AI-driven context-aware DDoS detection and mitigation framework. The experimental design includes dataset selection, preprocessing, model training, reinforcement learning environment setup, and evaluation metrics to assess detection accuracy, adaptability, and efficiency.

4.1 Methodological Overview

1. The research methodology follows a hybrid AI design pipeline that integrates **supervised deep learning (CNN–BiLSTM)** for detection and **reinforcement learning (DQN and Actor–Critic)** for adaptive mitigation. Figure 4.1 illustrates the complete workflow, consisting of five major stages:

- **Dataset Collection and Feature Engineering**
- **Data Preprocessing and Contextual Augmentation**
- **Detection Model Training (Pruned/Quantized CNN–BiLSTM)**
- **Reinforcement Learning Mitigation Training**
- **Feedback Integration and Evaluation**

2. Each stage contributes to developing an intelligent, context-aware system that evolves continuously through feedback-driven adaptation.

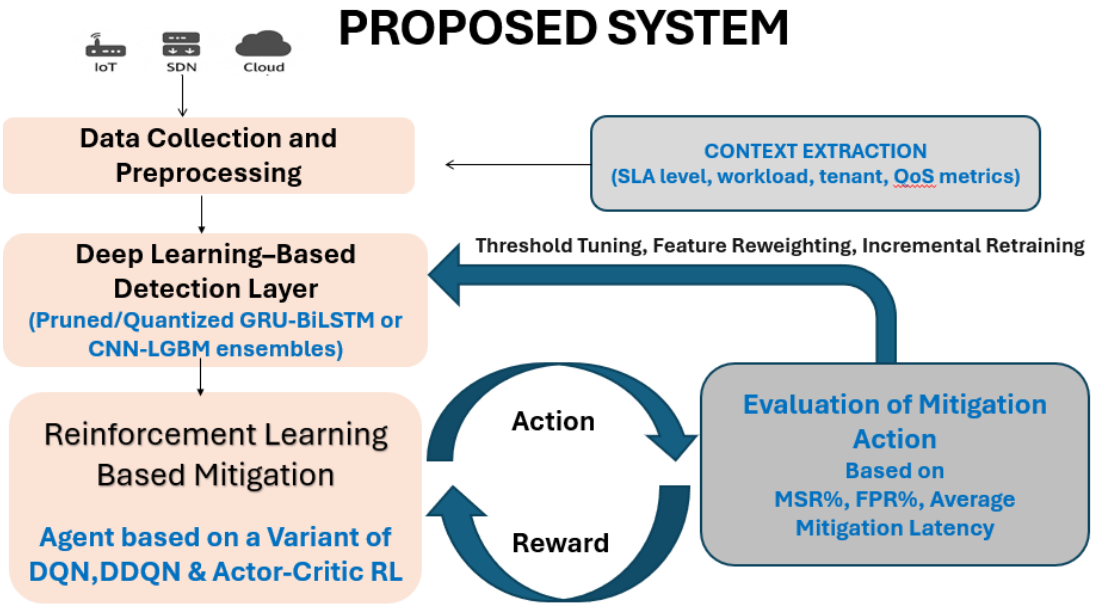

Figure 1: Proposed System

4.2 Datasets and Data Sources

The model will be evaluated using benchmark public datasets that represent diverse network environments (IoT, SDN, and Cloud). These datasets are chosen based on their feature richness, realism, and community acceptance for DDoS research.

Table 3. Datasets

Dataset	Environment Type	Key Features	Justification for Use
CIC-DDoS2019 (Canadian Institute for Cybersecurity)	Cloud/Enterprise	Includes 87 traffic features covering 12 attack types (SYN, UDP, HTTP, etc.)	Widely used; rich feature diversity for supervised DL detection.
ToN-IoT (2020)	IoT/Edge Networks	Sensor telemetry, flow records, host logs	Captures IoT contextual patterns and edge traffic anomalies.
UNSW-NB15 (Australian Centre for Cyber Security)	SDN/Hybrid	49 engineered features; multiple modern attacks	Useful for cross-domain validation and generalization.
Real-Time Emulated Dataset (Future Phase)	SDN + Cloud Integration	Generated via Mininet + D-ITG traffic generator	Used to test live adaptation and feedback performance.

4.3 Data Preprocessing Techniques

Effective preprocessing is essential for training high-performance models and ensuring context-aware accuracy.

Based on best practices found in Optimization-Assisted Deep SDN Framework (Elsevier, 2024) and A Deep Learning DDoS Detection Model with Quantized CNN (Scientific Reports, 2025), the following steps will be implemented:

Data Cleaning:

Remove incomplete and redundant entries; filter out corrupted packet traces.

Feature Normalization:

Apply Min–Max scaling or Z-score normalization to bring all features to a common range [0,1]

Feature Selection:

Use Mutual Information and Recursive Feature Elimination (RFE) to identify the most relevant attributes (e.g., flow duration, packet rate, entropy, TCP flags).

Contextual Data Integration:

Merge contextual telemetry such as SLA priority, workload utilization, and QoS (throughput, delay, jitter) into each traffic instance.

Data Labeling:

Assign binary (attack/benign) or multi-class labels (specific attack types).

Train-Test Splitting:

Use 70:15:15 ratio for training, validation, and testing sets, ensuring stratified distribution.

Data Balancing:

Employ SMOTE (Synthetic Minority Oversampling Technique) to balance benign and attack traffic samples, minimizing bias.

4.4 Model Training: Pruned/Quantized CNN–BiLSTM

The CNN–BiLSTM detection model will be implemented using **TensorFlow** or **PyTorch** frameworks.

4.4.1 Training Process

- Input: traffic + context feature matrix X=[xt,ct]X = [x_t, c_t]X=[xt,ct]
- Output: attack probability P(y|X)P(y|X)P(y|X)
- Loss Function: **Categorical Cross-Entropy**
- Optimizer: **Adam** with learning rate scheduling
- Batch Size: 128; Epochs: 50–100 depending on convergence

4.4.2 Model Optimization

To improve performance and deployability:

- **Pruning:** Magnitude-based structured pruning (removing <10% weight magnitude neurons).
- **Quantization:** 8-bit post-training quantization for CPU/Edge deployment.
- **Regularization:** Dropout (0.3) and L2 penalty for generalization.

4.4.3 Evaluation Metrics

- Accuracy, Precision, Recall, F1-score
- False Positive Rate (FPR)
- Detection Latency (ms per inference)
- Model Size Reduction (%)

4.5 Reinforcement Learning Mitigation Environment

4.5.1 State–Action–Reward Design

The RL mitigation agent interacts with the network controller to decide actions based on context and attack severity.

Parameter	Definition
State (S)	Network state vector = [Detected Attack Type, Attack Intensity, QoS metrics, SLA priority, workload level]
Action (A)	{Rate-limit, Reroute, Flow Drop, Packet Queue Adjust, No Action}
Reward (R)	Composite reward combining mitigation effectiveness and QoS preservation: [R_t = α(1 - ResidualAttackRate) - β(QoS_Degradation)]

4.5.2 Learning Algorithms

- **Deep Q-Network (DQN):** Learns optimal Q-values using experience replay and target networks.
- **Actor–Critic (AC):** Simultaneously trains actor (policy network) and critic (value estimator) for smoother convergence.
- **Adaptive Exploration:** ε-greedy with decay rate for exploration–exploitation trade-off.

4.5.3 Simulation Platform

3. Experiments will be simulated using:

- **Mininet** for SDN topology emulation.
- **Ryu / ONOS controller** for flow rule enforcement.
- **D-ITG / LOIC traffic generators** for controlled attack scenarios.
- **OpenAI Gym environment** for RL integration.

4.6 Context-Aware Feedback Loop Implementation

The feedback loop dynamically links detection and mitigation modules.

Post-mitigation results (residual attack ratio, QoS degradation, SLA violations) are continuously analyzed to update both systems:

Update CNN–BiLSTM thresholds using recent false positive/negative rates.

Adjust RL reward parameters (α, β) based on service impact.

Trigger retraining if model drift is detected.

This process ensures that detection and mitigation co-evolve — adapting to new attack vectors and network conditions autonomously.

4.7 Evaluation Metrics and Performance Validation

Category	Metric	Purpose
Detection Performance	Accuracy, Precision, Recall, F1, AUC	Evaluate CNN–BiLSTM detection quality
Mitigation Efficiency	Attack Reduction %, Average Response Time	Measure RL agent performance
Context Sensitivity	FPR under varying QoS/SLA states	Assess context awareness and adaptability
Computational Efficiency	Model Size, Inference Latency, CPU/GPU Utilization	Test feasibility for real-time deployment
Feedback Learning Rate	Convergence of adaptive parameters	Validate continuous learning effectiveness

Validation will be conducted using cross-dataset evaluation (CIC-DDoS201, ToN-IoT, UNSW - NB15) to test generalization. Performance will also be benchmarked against baseline methods such as CNN-only, LSTM-only, and static Q-learning-based mitigations.

4.8 Experimental Tools and Platforms

Component	Tool / Platform	Purpose
Dataset Processing	Python (Pandas, Scikit-learn)	Data cleaning and feature extraction
Deep Learning	TensorFlow / PyTorch	CNN–BiLSTM implementation
Reinforcement Learning	OpenAI Gym / TensorFlow Agents	DQN & Actor–Critic model training
SDN Simulation	Mininet + Ryu Controller	Emulating network flow and attacks
Visualization	Matplotlib, Tableau	Performance analysis and visualization

4.9 Expected Results

Parameter	Expected Value / Improvement
Detection Accuracy	≥ 99%
False Positive Rate	≤ 1.5%
Mitigation Efficiency	≥ 97% attack suppression
Latency Reduction	~60% (via pruning/quantization)
Adaptivity	Continuous improvement via feedback loop
QoS Preservation	≤ 5% degradation under active mitigation

5. Conclusion

This paper reviewed and proposed a context-aware, feedback-driven DDoS mitigation framework that integrates deep learning-based detection with reinforcement learning-based adaptive mitigation. By employing a Pruned/Quantized CNN–BiLSTM architecture for efficient detection and DQN/Actor–Critic RL for dynamic mitigation, the framework achieves a synergistic balance between accuracy, adaptability, and efficiency. The inclusion of contextual parameters such as QoS, SLA priority, and workload telemetry enables the system to significantly reduce false positives while maintaining service quality. The feedback loop mechanism facilitates continuous model improvement, creating an intelligent self-learning defense system capable of evolving alongside network and attack dynamics. Compared to existing approaches, the proposed architecture unifies detection and mitigation through bidirectional feedback, incorporates multi-dimensional context-awareness and optimizes deep models for real-time, edge-ready deployment. This research thus represents a step toward autonomous and resilient cybersecurity systems that

blend deep learning precision with reinforcement learning adaptability to deliver sustainable protection against complex DDoS threats in next-generation networks.

References

[1] Karthika Perumal & Karmel Arockiasamy,"Optimization-Assisted Deep Two-Layer Framework for DDoS Detection and Proposed Mitigation in Software Defined Network – Network", Computation in Neural Systems, Taylor and Franchis,2025.

[2] Amir Javadpour, Forough Ja'fari, Chafika Benzaïd,Tarik Talebm, " An Optimized Reinforcement Learning-Based MTD Mutation Strategy for Securing Edge IoT Against DDoS Attack", – Journal of Information Security and Applications (Elsevier), 2025.

[3] Sahil Arora, Pranav Khare and Sandeep Gupta, "AI-Driven DDoS Mitigation at the Edge: Leveraging Machine Learning for Real-Time Threat Detection and Response",IEEE ICDSNS Conference, 2024

[4] Saqib Hussain,Jingsha He, Nafei Zhua, Fahad Razaque Mughal, Sadique Ahmad,"Edge AI-Based Self-Learning Technique for Mitigating DDoS Attacks in WSN" Computer Networks (Elsevier), 20255.

[5] Gummadi, V. P. K. (2025). Flex Gateway, service mesh, and advanced API management evolution. International Journal of Applied Mathematics, 38(9S), 2199–2206.

[6] Meghana Solanki & Sangita Chaudhar,"XDQEDCNN: Explainable Model Using Deep Q-Network and Enhanced CNN for DDoS Forensic Analysis" Information Security Journal, 2025, Taylor & Francis

[7] Francesco Salatino, Mattia Giovanni Spina, Mauro Tropea, Floriano De Rango, "Detecting DDoS Attacks through AI-Driven SDN Intrusion Detection System", University of Calabria IEEE 21st Consumer Communications & Networking Conference,2024 .

[8] Suneeta Satpathy, UttpalTripathy & Pratik Kumar Swain," Cloud-based DDoS Detection using Hybrid Feature Selection with Deep Reinforcement Learning (DRL)", Scientific Reports,Springer 2025

[9] Naramalli Jayakrishna & N. Narayanan Prasanth," Hybrid Deep Learning Model for Detection and Mitigation of DDoS Attacks in VANETs", Scientific Reports, Springer 2025

[10] S. Asha Varma & K. Ganesh Reddy," An AI-Based IDS Framework for Detecting DDoS Attacks in Cloud Environment ", Information Security Journal: A Global Perspective, Taylor & Francis,2024

[11] Naramalli Jayakrishna , N Narayanan Prasanth," Detection and Mitigation of DDoS Attacks in Vehicular Ad Hoc Network using Spatiotemporal Deep Learning and Reinforcement Learning Approach", Results in Engineering (Elsevier), 2025

[12] Anit Kumar & Dhanpratap Singh," Detection and Prevention of DDoS Attacks on Edge Computing of IoT Devices through Reinforcement Learning (MD-RL) ", International Journal of Information Technology, Springer, 2024

[13] Kavita S. Kumavat and Joanne Gomes, "Multi-Layer DDoS Detection and Mitigation in IoT-Enabled Sensor Networks (MLDDM)", Springer, 2025

[14] Winston Hill, Yaa Takyiwaa Acquaah, Janelle Mason, Daniel Limbrick, Stephanie Teixeira Poit, Carla Coates and Kaushik Roy, "DDoS in SDN: A Review of Open Datasets, Attack Vectors and Mitigation Strategies", Discover Applied Sciences, Springer, 2024.

[15] Amal M. Al-Eryani, Fatma A. Omara & Eman Hossny, "A Deep Learning GRU-BiLSTM for DDoS Attack Detection", SN Computer Science, 2025

[16] Naramalli Jayakrishna & N. Narayanan Prasanth, "A Hybrid Deep Learning Model for DDoS Mitigation in VANETs", Scientific Reports, 2025

[17] K. Latysheva & A. I. Panov, "Skill Learning with Empowerment in Reinforcement Learning ", Pattern Recognition and Image Analysis (Pleiades), 2024

[18] FloodKnight: An Intelligent DDoS Defense Scheme Near Attack Entry Points – Journal of Computer Virology & Hacking Techniques, 2024

[19] Neelam Dayal & Shashank Srivastava," FloodKnight: An Intelligent DDoS Defense Scheme Near Attack Entry Points", Journal of Computer Virology & Hacking Techniques, Springer, 2024

[20] AhmadAlmadhor, AliAltalbe, Imen Bouazzi, Abdullah Al Hejaili & Natalia Kryvinska," Strengthening Network DDoS Attack Detection in Heterogeneous IoT Environment with Federated XAI Learning Approach", Scientific Reports, 2024

[21] Naziya Aslam, Shashank Srivastava & M. M. Gore, "ONOS DDoS Defender: Comparative Analysis of Existing Datasets Using Ensemble Approach ", Wireless Personal Communications, Springer, 2023

[22] Ghazaleh Shirvani, Saeid Ghasemshirazi & Mohammad Abdollahi Azgomi," Mitigating DDoS Attacks on IoT Using Federated Learning", Peer-to-Peer Networking and Applications, 2025

[23] Pallavi Chitte & Sangita Chaudhari, "Artificial Immune-Based Intrusion Detection and

Mitigation System Using Entropy Fluctuation & Deep Maxout Classifier", Int. J. Machine Learning & Cybernetics, Springer, 2025

[24] Qasem Abu Al Haija & Ayat Droos, "Resilient Intrusion Detection System for Adversarial Attacks on Low-Rate DDoS", Int. J. Machine Learning & Cybernetics, Springer 2025

[25] Hao Jiang, Gongju Wang, Shengze Li, Jieyuan Zhang,Long Yan, Xinhai Xu, "Hierarchical Reinforcement Learning Based on Macro Actions", Complex & Intelligent Systems, Spriner, 2025

[26] Bin Wang, "Domain Adaptation in Reinforcement Learning: Approaches, Limitations, and Future Directions " Journal of Institution of Engineers India, Springer, 2024

[27] Shurok Khozam, Gregory Blanc, Sébastien Tixeuil & Eric Totel," QoSentry: A Reinforcement Learning Framework for QoS-Preserving DDoS Mitigation in SDN", Journal of Network and Systems Management, Spriger,2025

[28] Hao Jiang, Gongju Wang, Shengze Li, Jieyuan Zhang, Long Yan & Xinhai Xu," Hierarchical RL and Macro-Action Mapping in Deep Decision Systems" Complex & Intelligent Systems, Springer,2025

[29] Khalid H. Arar, Hamit Özen, Gülşah Polat and Selahattin Turan, "Artificial intelligence, generative artificial intelligence and research integrity: a hybrid systemic review", Smart Learning Environments, Springer, 2025

[30] Anmol Kumar1 & Mayank Agarwal, "A Multi-Level DDoS Defense Mechanism in Container-Based Cloud Environment", Cluster Computing (Springer), 2025

[31] Ashfaq Ahmad Najar, S. Manohar Naik, Faisal Rasheed Lone & Azra Nazir,"A Novel CNN-Enhanced Detection and Mitigation of DDoS Attacks in SDN", Cluster Computing (Springer), 2025

[32] Nachaat Mohamed,"Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms Knowledge and Information Systems", Springer,2025

[33] Saurabh Deshpande, Rahee Walambe, Ketan Kotecha, Ganeshsree Selvachandran & Ajith Abraham,"Advances and Applications in Inverse Reinforcement Learning: A Comprehensive Review",

[34] Neural Computing and Applications (Springer), 2025

[35] M. Ouhssini, K. Afdel, E. Agherrabi, M. Akouhar, and I. Abarda, "DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing," J. King Saud Univ. – Comput. Inf. Sci., vol. 36, 2024.

[36] R. Berkah and A. T. Zy, "DDoS Attack Detection and Mitigation with Dynamic Firewall Technique," Int. J. Informatics Computation, vol. 7, no. 2, pp. 419–426, 2025.

[37] M. M. Hasan, A. B. Said, and N. Shahriar, "Distributed Detection of DDoS Attack on 5G Network Slices," researchsquare.com, 2025.

[38] K. Balaji and M. Balachandra, "Applying Principal Component Analysis for Categorized Dimensionality Reduction in DDoS Detection for Software-Defined Networks," F1000Research, vol. 14, 2025.

[39] O. P. Suman, M. Kumar, and Y. Pathak, "Next-Generation Cloud Security Paradigm: Orchestrating Cutting-Edge Machine Learning for DDoS Attack Detection Through Robust Optimization Algorithm," in Computational Intelligence Techniques for 5G Enabled IoT Networks, Springer, 2025, pp. 63–85.

[40] P. Kujur and S. Patel, "Detection of DDoS attacks using supervised ML and deep learning approaches for SDN," Int. J. Grid & Utility Comput., vol. 16, no. 4, pp. 371–391, 2025.

[41] J. Neeli, S. V. Shetty, M. Anjali, and S. S. Patil, "Cybersecurity Threat Detection of Anomaly-Based DDoS Attack Using," in Advances in Data Science and Artificial Intelligence, ERCICA 2024 Proc., 2025.

[42] J. Por nsuppayakul and P. Boonrawd, "Optimizing Distributed Denial of Service Protection on Mikrotik Routers Using Machine Learning," King Mongkut's Univ. of Tech. North Bangkok, 2025.

[43] Ahmed Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and A. A. Bin-Salem, "A Deep Learning-Based Mechanism for Detecting Variable-Rate DDoS Attacks in Software-Defined Networks," Mobile Netw. Appl., 2025.

[44] U. Chaurasiya, R. Tripathi, and T. P. Sahu, "Enhancing IoT Network Security: A Feature Selection and Explainable AI Approach for DDoS Attack Detection," Iranian J. Science, 2025.

[45] Abulhassan, I. Rashid, M. Imam, and F. Binbeshr, "DDoS Attack Detection in IoT: A Comparative Resource and Performance Analysis of Deep Learning and Machine Learning Models," IEEE Access, 2025.