International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A HYBRID FRAMEWORK FOR DETECTION AND MITIGATION OF DDOS ATTACKS IN IOT ENVIRONMENT

T. Ramya[1*], Dr. A. Prasanth Rao[2]

[1*]Research Scholar, Department of Information Technology, Anurag University, Hyderabad, Telangana-500088.
[2]Professor, Department of Information Technology, Anurag University, Hyderabad, Telangana-500088.

Abstract

Internet of Things (IoT) devices are becoming increasingly valuable, but they moreover come with more security dangers and vulnerabilities because of their constrained assets. Distributed Denial of Service(DDoS) could be a noteworthy peril to IoT gadgets. This paper presents a novel learning design for distinguishing and mitigating DDoS attacks in IoT systems. It uses a Robust covariance-based Principal Component Analy- sis (RCPCA) technique for pre-processing, which successfully identifies and removes outliers from the complex IoT network traffic data. The Lyrebird Armadillo Fusion Algorithm (LAFA), which combines the Lyrebird Optimization Algorithm (LOA) with the Giant Armadillo Optimization (GAO), is used by the framework to select optimal features. The Proposed Framework presents the Capsule Gated Perception (CGP) model, a deep learning model that combines an optimized Multi-Layer Perceptron (MLP), Gated Repetitive Units (GRU), and Capsule Systems for the purpose of assault discovery. In conclusion, the proposed framework employments Profound Q-Networks (DQN) to mitigate assaults by reacting to DDoS assaults in real- time and reinforcing the security and flexibility of IoT systems.

Index Terms—Cyber Attack, Internet of Things, Detection, Mitigation

I. INTRODUCTION

In today's fast-developing ecosystem of automated and linked gadgets, the whole universe is assumed as a vast network of gadgets that are connected and interact. It is the IoT device, a ubiquitous computer network that enables actuators and sensors to communicate with living objects and non-living items, that can link all of those "objects" to the Internet. But as the network expands, so do the Several works [1], [2] proposed deep learning-based DDoS detection. The future of the domain is significantly impacted by IoT security issues, which raise questions about the security of currently in-use devices. In the meantime, DDoS (DDoS) attacks are becoming more and more common in the field of cybersecurity [3], [4]. When objects are connected via the Internet, DDoS attacks have increased significantly. Given that there are more devices available to attack and hack. Attackers now have an easier time breaking into IoT scenarios due to the resource-constrained platforms they use. In the realm of IoT defense, all of these research topics have grown recently. The IoT is made up of several devices with different features and functions [5], [6], [7]. High-end computer systems and simple microprocessors with limited memory and processing power are among the different types. In this diversified atmosphere, security solutions must also be developed at many levels. The scope and characteristics of implementing security controls at every IoT tier can vary due to the differences in device capabilities. Generally speaking, there are several DDoS, denial of service (DoS), and MITM assaults that lead to the failure of different IoT devices [8], [9], [10]. Physical objects that are capable of being connected to the Web and distinguishing themselves from different gadgets are known as the IoT. (IoT). IoT devices are closely related to RFID, sensor technologies, and developments in remote computing [11], [12], [13]. It enables the use of an already-existing device framework to identify and monitor items remotely. The World Wide Web is a global network that facilitates global communication through

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

messaging, gaming, conferencing, and web-based information sharing. The universal objects share the capacity for planning, extensive inspection, and information dissemination. In this context, ”intelligent” refers to a role that is deemed necessary. The intelligent IoT enables distributed smart elements including sensors, actuators, and information centers [14], [15]. Therefore, it is important to highlight that denial-of-service attacks are becoming more common and can be used purposefully for a variety of advantages. Security is currently a top priority Owing to the multiple vulnerabilities of IoT equipment and an immediate increase in DDoS types. A few sorts of investigations and studies have been conducted to create arrangements to relieve these concerns and secure IoT gadgets and the arrange from being compromised. The essential commitments of the paper are as follows, to effectively perform the pre-processing process, the RCPCA model is introduced. The Covariance is calculated along with the normal PCA to effectively identify and eliminate outliers.

- The proposed framework integrates various feature ex- traction techniques including time-series analysis, frequency domain analysis, database feature extraction, statistical feature computation, and entropy-based feature extraction.
- To improve the feature selection process, the paper utilizes the Lyrebird Armadillo Fusion Algorithm (LAFA) for feature selection, which combines the Lyrebird Optimization Algorithm (LOA) and the Giant Armadillo Optimization (GAO).
- The proposed framework introduces a novel Capsule Gated Perception (CGP) model, which amalgamates Capsule Networks, Gated Recurrent Units (GRU), and an optimized Multi-Layer Perceptron (MLP). This synergistic approach enhances the accuracy and robustness of attack detection.

Following that, the remaining proposed work is arranged in order: A DDoS attack scenario in an IoT network in existing papers is briefly described in Section 2. The proposed archi- tecture, model training dataset, attack detection architecture, and mitigation techniques are all introduced in Section 3. The results of the suggested strategy and the results of the existing technique are compared in Section 4. Section 5 concludes by summarizing the work.

II. Literature Review

In 2023, Khedr et al. [16] suggested a multi-layer machine learning-based framework for stateful SDN-based IoT systems to identify and relieve DDoS assaults. The proposed FMDADM plan comprises five levels and four essential components. The primary unit employs a normal drop rate (ADR)–based early detection approach with a window size of 32 packets. The secondary module utilizes a double-check mapping function (DCMF) to assist within the early detection of assaults at the data plane level. The third module executes an ML-based detection program using SVM, kNN, DT, RF, BLR, and GNB models. A process for mitigating attacks is introduced in the last module.
In 2023, Ahmim et al. [17] presented a hybrid deep learning approach for identifying DDoS assaults within the IoT. The study introduces a new hybrid deep learning model that integrates several deep neural network types: CNN, LSTM, Deep Autoencoder, and DNN. The main goal was to produce a high-performing model by leveraging the diverse properties of various deep neural network types through integration. These outcomes were achieved using a dataset that comprises a variety of DDoS attack kinds, including the most common and comparable ones.
In 2023, Elubeyd and Yiltas-Kaplan [18] recommended a hybrid deep learning technique for Software-Defined Net- works (SDN) automatic detection of DoS/DDoS assaults. The study shows that using deep learning procedures to distinguish and defend against DDoS assaults in SDN systems was a successful strategy. The suggested hybrid deep learning model, which incorporates a GRU, a DNN, and a 1D CNN, has demonstrated better performance than conventional ma- chine learning algorithms in terms of properly identifying DDoS attacks and ensuring the smooth

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

operation of SDN networks. However, no mitigation strategies were included. In 2022, Sattari et al. [19] presented a hybrid deep learning strategy for IoT botnet detection. It introduces a modern strategy for identifying botnet assaults that may be used in mist computing scenarios to mitigate the attack by leveraging the SDN environment's programmable features. Three hybrid models were employed in the creation of the botnet detection framework. Based on the evaluation, the hybrid DNN-LSTM model successfully identified device and Mirai botnets within
the N_BaIoT scenario with the highest accuracy.

In 2024, Yaras and Dener [20] suggested a novel hybrid deep learning algorithm for an IoT-based intrusion detection system. LSTM and one-dimensional CNN were used to create the hybrid deep learning method. Ten deep learning and machine learning methods were compared to the developed approach. A substantial amount of data was required to obtain high accuracy. Training and testing times were prolonged due to the large amount of data. In real life, it is critical to identify attack traffic such as DDoS that necessitates quick action and effective use of system resources. By optimizing training and creating intrusion detection systems that were inexpensive and highly accurate, their work addressed this challenge.

In 2022, Alzahrani and Bamhdi [21] utilized a hybrid deep learning model for IoT environments to detect botnet attacks. This was achieved by combining a long short-term memory (LSTM) mechanism with a convolutional neural network (CNN) to detect two predominant and harmful IoT attacks (BASHLITE and Mirai) on four different types of security cameras. The hybrid model proved effective in detecting botnet attacks that compromised IoT camera devices. The system was developed to intelligently identify major IoT threats and can also detect unknown botnet infections.

In 2022, Ali et al. [22] performed a threat analysis and identified DDoS assaults within IoT networks. The paper examined threats and intrusion activities using evolutionary sparse convolution networks (ESCNNs). The dataset used was the DDoS Evaluation Dataset. Training, testing, and validation data were derived from it. To improve detection ac- curacy, the data was processed using multiple levels of long- term and short-term systems. Testing details were categorized using feature extraction and sparse matrix construction. This method enhanced detection accuracy while keeping false alarms low.

In 2022, Kumar et al. [23] recommended a distributed intrusion detection solution for blockchain-enabled IoT systems to detect DDoS assaults. The proposed distributed IDS utilized mist computing to detect DDoS attacks over the mining pool in blockchain-supported IoT networks. Performance was evaluated using Random Forest (RF) and Extreme Gradient Boosting (XGBoost) on distributed mist nodes. The approach was validated on the BoT-IoT dataset, which includes recent attacks observed in blockchain-enabled IoT systems.

In 2022, Brindha Devi et al. [24] investigated IoT threat detection and mitigation using deep learning approaches. Their DL-oriented method used multiple classifiers, including Recurrent Neural Network (RNN), Bidirectional GRU (BI-GRU), and Bidirectional LSTM (BI-LSTM). The Bi- LSTM weights were fine-tuned with Cat and Mouse Coordinates HBO (CMIHBO). However, the work raised concerns about how the system might respond to privacy and QoS constraints.

In 2022, Reddy and Shyam [25] introduced a secure SaaS system with machine learning for threat detection and mitigation. The main contribution was an attack detection method using Deep Belief Networks (DBN), optimized with the Ocean Lion Optimization algorithm. When an attack node was detected, the system redirected traffic using a lightweight honeypot method, effectively mitigating the most common attack nodes without disrupting legitimate traffic.

Figure axis labels are often a source of confusion. Use words rather than symbols. As an example, write the quantity ”Magnetization,” or ”Magnetization M,” not just ”M.” Put units in parentheses. Do not label axes only with units.

Large figures and tables may span both columns. Place figure captions below the figures; place table titles above the tables. If your figure has two parts, include the labels ”(a)” and ”(b)” as part of the artwork. Please verify that the figures and tables you mention in the text actually exist.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

III. Proposed Methodology

The proposed methodology provides a new strategy for identifying and mitigating DDoS assaults in IoT networks. The framework extracts many features, including time-series analysis, frequency domain analysis, database feature ex- traction, statistical feature calculation, and entropy-based feature extraction. It starts with pre-processing the data using RCPCA to find outliers. The Lyrebird Armadillo FusionAlgorithm is used for feature selection, producing a more useful subset of features for attack detection. For reliable attack detection, the innovative CGP model integrates GRU,an improved MLP, and capsule networks. Finally, the DQN model is utilized for intrusion mitigation. Figure 2 illustrates the well-defined process of the suggested attack mitigation model.

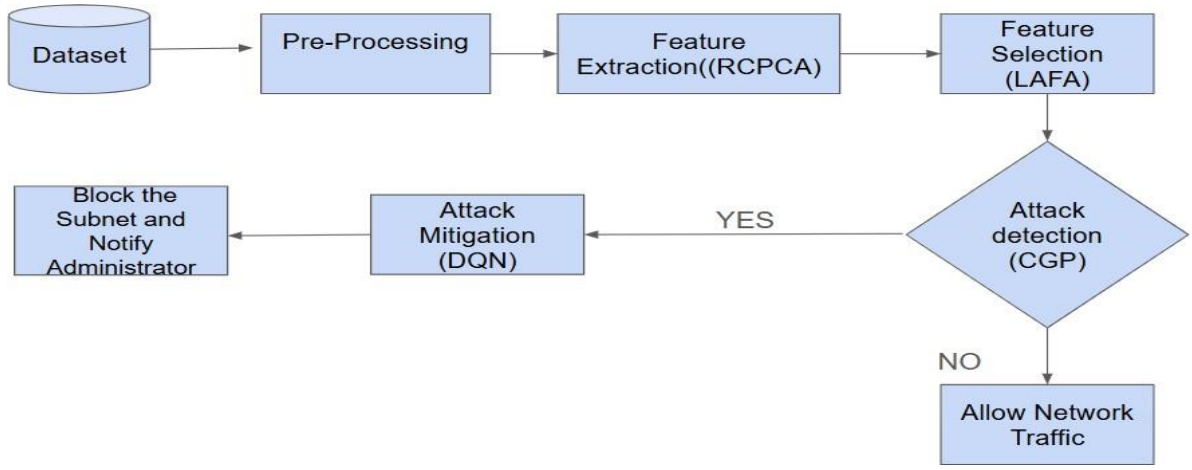

Fig. 1. Block representation of the Intrusion detection and mitigation model

A. Pre-processing

The input data is collected from two datasets, which are pre-processed using the RCPCA model. By using the RCPCA technique, the outliers present in the input data are removed.

1) ***Data Collection:*** **This work utilized two datasets, which are given as follows:**

- **Dataset 1: DDoS Botnet Attack on IoT Devices** This is a collection of IoT-related DDoS Botnet assaults. It includes all functionality related to bot-generated packets [26].
- **Dataset 2: APA-DDoS Dataset**

The number of linked devices is growing exponentially, making it harder to identify malicious connections. One common technique used for this purpose is IDS. With the advancement of the assaults, machine learning is widely applied in intrusion detection systems. ML tools must have access to attack patterns that reflect all types of traffic. Unfortunately, not every pattern for known attacks is available in public datasets. This project aims to bridge that gap, especially for underrepresented attacks such as ACK and PUSH-ACK flooding.

2) ***Outlier Detection and Removal using RCPCA:*** When working with data that contains outliers or corrupted values, PCA is known to be unstable. Because PCA tries to capture as much variance as possible in the first few principal components, it skews the results in favor of the outlier. Outliers can have a critical effect on the variance of the data. In networks of low-cost nodes where noise, tampered values, or outliers are highly likely, this fragility poses a significant limitation. RPCA is a solution to PCA's shortcomings. Using this technique, X decomposes as

$$X = L + S$$

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

where S is a sparse matrix that gathers outliers and noise, and L represents a structured low-rank approximation of X. Principal component pursuit solves a convex relaxation of the underlying problem to find the matrices L and S:

$$\min_{L,S} \|L\|_* + \lambda\|S\|_1 \quad \text{subject to } X = L + S$$

Here, $\|L\|_*$ denotes the nuclear norm (sum of singular values) representing a matrix's rank, and $\|S\|_1$ is the l_1- norm. The parameter λ balances both terms. According to the original RPCA article, the ideal value is

$$\lambda = \frac{1}{\sqrt{\max(n, m)}}$$

With the assumption that L is not sparse and S is not low- rank, the solution of Eq. (2) converges towards the genuine optimal solution with high probability. After determining L and S, the matrix L is decomposed using singular value decomposition:

$$L = U\Sigma V^T$$

3) Standard PCA: How PCA functions is as follows: let

$$X = [x_1, x_2, \ldots, x_m] \in \mathrm{R}^{N\times m}$$

represent a data matrix with m features and N samples. The mean-centered matrix is

$$\bar{X} = X - \mu_X$$

where μ_X is the feature mean vector. The sample covariance matrix $C \in \mathrm{R}^{m\times m}$ of X is defined a

$$C = \frac{\bar{X}^T\bar{X}}{n-1}$$

Being symmetric, C can be diagonalized as

$$C = V\Lambda V^T \qquad (4)$$

where V is the set of eigenvectors of C, and Λ is the diagonal matrix of eigenvalues λ_i, sorted in decreasing order. The principal components of X are defined by $\bar{X}\ V$. The largest eigenvalues correspond to directions of maximum variance, also known as explained variance.

B. Feature Selection with Hybrid LAFA Optimization

Distributed Denial of Service (DDoS) attacks pose a severe threat to IoT environments. Traditional machine learning approaches often struggle with high-dimensional data and a wide range of features. Differentiating between relevant and irrelevant features becomes difficult, leading to higher false positives.

To address this, we propose a hybrid optimization model that combines the Giant Armadillo Optimization (GAO) algorithm and the Lyrebird Optimization Algorithm (LOA). GAO's adaptive exploration and exploitation behavior, combined with LOA's dynamic mimicry-based search behavior, helps in selecting the optimal feature subset. This improves classifier performance, reduces false positives, and ensures scalability in resource-constrained IoT networks.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The pseudocode of the proposed LAFA model is presented below.

Initialize population P
$best\_solution \leftarrow$ None
$best\_fitness \leftarrow \infty$
for $i = 1$ to $epochs$ **do**
  for $j = 1$ to pop_size **do**
    $P[j] \leftarrow clamp(P[j], lb, ub)$
    $fitness \leftarrow Objective\_function(P[j])$
    if $fitness < best\_fitness$ **then**
      $best\_solution \leftarrow P[j]$
      $best\_fitness \leftarrow fitness$
    end if
    $r_p \leftarrow \text{rand}(0, 1)$
    if $r_p < 0.5$ **then**
      Select STM from candidate solutions
      $I \leftarrow \text{rand}(1, 2)$
      $P[j] \leftarrow P[j] + \text{rand}(0, 1) \times (STM - I \times P[j])$
    else if $r_p = 0.5$ **then**
      $R \leftarrow 0.01$
      $P[j] \leftarrow P[j] + R \times (2 \times \text{rand}(0, 1) - 1) \times (1 - \frac{i}{epochs}) \times P[j]$
    else
      $P[j] \leftarrow P[j] + (1 - 2 \times \text{rand}(0, 1)) \times \frac{ub - lb}{i}$
    end if
  end for
end for
return $best\_solution$, $best\_fitness$

Fig. 2. Pseudocode of the Proposed LAFA Model

C. Detection Model: Capsule–GRU–Perceptron (CGP)

The proposed detection framework combines three complementary components: Gated Recurrent Units (GRU), Capsule Networks (CapsNet), and a Multi-Layer Perceptron (MLP). This hybrid design leverages the strengths of each model to improve intrusion detection performance in IoT networks.

1) Temporal Learning with GRU: The GRU is employed to capture temporal dependencies in network traffic. Since IoT attacks often exhibit sequential patterns across packets and flows, GRU efficiently learns these dependencies using its update and reset mechanisms. Unlike traditional recurrent models, GRU is computationally lightweight and suitable for resource-constrained environments.

2) Hierarchical Representation with Capsule Networks: Capsule Networks are used to preserve spatial relationships and feature hierarchies. In intrusion detection, features extracted from traffic are not independent but follow hierarchical patterns. CapsNet groups features into capsules that represent both the presence of a pattern and its orientation. Through dynamic routing, the network ensures that relevant patterns are emphasized while irrelevant variations are suppressed, providing robust representation of malicious behaviors.

3) Classification with MLP: The fused features from GRU and CapsNet are passed into a Multi-Layer Perceptron. The MLP acts as the final decision-making module, performing non-linear transformations and mapping the learned representations into attack or benign categories. The MLP is flexible, scalable, and ensures fast classification suitable for real-time detection.

4) Advantages of the Hybrid Approach: By integrating GRU, CapsNet, and MLP, the proposed CGP model offers several advantages:

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- GRU captures sequential dependencies in attack traffic.
- CapsNet preserves hierarchical feature structures and spatial relationships.
- MLP performs efficient final classification with strong generalization capability.

This combination ensures that both temporal and structural properties of IoT traffic are leveraged, resulting in improved detection accuracy, reduced false positives, and greater robustness against evolving DDoS attack strategies.

IV. MITIGATION USING DEEP Q-NETWORK (DQN)

Detection alone is not sufficient in securing IoT networks against Distributed Denial of Service (DDoS) attacks. Once malicious traffic is identified, it must be mitigated in real time to ensure service continuity. To achieve this, the proposed framework employs a Deep Q-Network (DQN) based mitigation strategy. DQN combines the principles of reinforcement learning with deep neural networks, enabling the system to learn adaptive and intelligent defense mechanisms.

A. Rationale for DQN-Based Mitigation

Conventional mitigation techniques, such as static rules or fixed thresholds, often fail when attackers change their strategies. DQN overcomes this limitation by learning directly from interactions with the environment. By continuously updating its policy, the agent adapts to new attack behaviors and ensures effective traffic management without human intervention.

B. System States

The network environment is modeled as a set of states that describe traffic conditions at a given time. These states may include traffic flow rates, protocol distributions, connection attempts, flagged anomalies, and resource utilization. Monitoring these states allows the agent to capture the dynamic nature of both normal and attack traffic in IoT environments.

C. Mitigation Actions

The DQN agent can take a variety of actions to counter malicious traffic. These include rate-limiting suspicious flows, blacklisting or quarantining compromised devices, rerouting traffic to honeypots, and dynamically updating firewall rules. By selecting appropriate actions, the agent ensures minimal disruption to legitimate users while blocking adversarial activity.

D. Learning Through Rewards

A reward mechanism guides the agent's learning process. Actions that successfully reduce attack impact while maintaining service quality yield positive rewards. In contrast, actions that block legitimate traffic or fail to mitigate an attack result in negative rewards. Over time, the agent learns to favor strategies that maximize long-term security and network performance.

E. Discussion on Table I

Table I compares the performance of different machine learning and deep learning models for Dataset 1 across multiple evaluation metrics, including Accuracy, Precision, Sensitivity, Specificity, F-Measure, MCC, NPV, FPR, and FNR.

The results show that traditional models such as CNN, DNN, and Bi-LSTM achieve good performance but fall short

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

TABLE I COMPARISON OF PERFORMANCE METRICS FOR DATASET 1

Metrics	CNN	DNN	BiLST	CNN+LST	RF+XGB	Prop
Accuracy	0.975	0.964	0.979	0.988	0.9814	**0.998**
Precision	0.977	0.961	0.979	0.988	0.9871	**0.997**
Sensitivity	0.971	0.967	0.978	0.982	0.9761	**0.999**
Specificity	0.978	0.960	0.979	0.989	0.9869	**0.998**
F-Measure	0.974	0.964	0.978	0.985	0.9816	**0.999**
MCC	0.950	0.928	0.958	0.977	0.9529	**0.982**
NPV	0.973	0.967	0.978	0.988	0.9757	**0.985**
FPR	0.021	0.039	0.020	0.011	0.0131	**0.001**
FNR	0.028	0.032	0.021	0.011	0.0239	**0.001**

compared to advanced hybrid approaches. The CNN+LSTM[20] model improves detection accuracy by capturing both spatial and temporal features. The RF+XGBoost [23] method also performs well, particularly in terms of accuracy and F- Measure.

However, the proposed CGP model significantly outperforms all baseline models across every metric. It achieves the highest Accuracy (0.9986), Precision (0.9978), Sensitivity (0.9999), and Specificity (0.9989). The F-Measure and MCC values are also substantially improved, reflect- ing the robustness of the approach. Importantly, the False Positive Rate (0.0011) and False Negative Rate (0.0001) are drastically reduced, demonstrating the reliability of the model in minimizing both false alarms and missed detections. Table II presents the comparison of performance

TABLE II COMPARISON OF PERFORMANCE METRICS FOR DATASET 2

Metrics	CNN	DNN	Bi-LST	CNN+LSTM	RF+XGB	Prop
Accuracy	0.973	0.960	0.977	0.987	0.981	**0.991**
Precision	0.955	0.943	0.964	0.983	0.972	**0.990**
Sensitivity	0.958	0.947	0.963	0.980	0.973	**0.990**
Specificity	0.980	0.976	0.982	0.990	0.986	**0.988**
F-Measure	0.956	0.943	0.968	0.985	0.972	**0.989**
MCC	0.940	0.919	0.946	0.971	0.958	**0.982**
NPV	0.953	0.974	0.986	0.990	0.982	**0.991**
FPR	0.020	0.029	0.018	0.009	0.013	**0.003**
FNR	0.040	0.058	0.036	0.019	0.028	**0.005**

metrics for Dataset 2 across different models, including CNN, DNN, Bi-LSTM, CNN+LSTM, RF+XGBoost, and the proposed approach. From the results, it is evident that the proposed model consistently outperforms the baseline methods across all evaluation criteria. The accuracy of the proposed model reaches 0.991, which is higher than all other models. Precision, sensitivity, specificity, and F- measure also record superior values of 0.990, 0.990, 0.988, and 0.989, respectively, reflecting its robustness in correctly identifying both positive and negative cases. Furthermore, the Matthews Correlation Coefficient (MCC) and Negative Predictive Value (NPV) are significantly higher at 0.982 and 0.991, respectively. Importantly, the proposed model achieves the lowest False Positive Rate (FPR) of 0.003 and False Negative Rate (FNR) of 0.005, which demonstrates its efficiency in reducing misclassifications. Overall, the table highlights that the proposed hybrid framework provides a more reliable and accurate solution for DDoS detection in IoT environments compared to conventional deep learning and machine learning approaches.

Overall, the proposed method establishes a clear advancement in DDoS detection for IoT environments, achieving near-perfect classification performance while ensuring practical applicability in real-world scenarios.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

V. Conclusion and Future Scope

In this work, an intelligent intrusion detection and mitigation framework for IoT networks vulnerable to DDoS attacks. The approach integrates a hybrid feature selection technique based on the Lyrebird–Armadillo Fusion Algorithm, ensuring that only the most relevant and discriminative features are retained. For detection, the Capsule–GRU–Perceptron (CGP) model was introduced, effectively combining temporal learning, hierarchical feature preservation, and robust classification to achieve superior accuracy and reliability. To complement detection, a Deep Q-Network (DQN) based mitigation strategy was incorporated, enabling adaptive and real-time response to evolving attack scenarios. Experimental analysis confirmed that the proposed framework consistently outperforms traditional machine learning and deep learning methods across multiple performance metrics, while maintains scalability for resource-constrained IoT devices.

Although the proposed system demonstrates excellent results , there remain opportunities for future work. Further research may explore lightweight and compressed model architectures to make deployment more feasible on ultra- constrained IoT nodes. Additionally, extending the framework to address a broader range of cyber threats beyond DDoS, and improving resilience against adversarial attacks, would strengthen its robustness.

References

[1] D. Akgun, S. Hizal, and U. Cavusoglu, "A new ddos attacks intrusion detection model based on deep learning for cybersecurity," *Computers & Security*, vol. 118, p. 102748, 2022.

[2] V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of ddos attacks on iot devices," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 1353–1374, 2022.

[3] S. Ahmed, Z. Khan, S. Mohsin, S. Latif, S. Aslam, H. Mujlid, M. Adil, and Z. Najam, "Effective and efficient ddos attack detection using deep learning algorithm, multi-layer perceptron," *Future Internet*, vol. 15, no. 2, p. 76, 2023.

[4] C. Kalutharage, X. Liu, C. Chrysoulas, N. Pitropakis, and P. Pa- padopoulos, "Explainable ai-based ddos attack identification method for iot networks," *Computers*, vol. 12, no. 2, p. 32, 2023.

[5] J. Almaraz-Rivera, J. Cantoral-Ceballos, and J. Botero, "Enhancing iot network security: Unveiling the power of self-supervised learning against ddos attacks," *Sensors*, vol. 23, no. 21, p. 8701, 2023.

[6] Y. Alhasawi and S. Alghamdi, "Federated learning for decentralized ddos attack detection in iot networks," *IEEE Access*, vol. 12, pp. 42 357–42 368, 2024.

[7] Avcı and M. Koca, "Predicting ddos attacks using machine learning algorithms in building management systems," *Electronics*, vol. 12, no. 19, p. 4142, 2023.

[8] T. Hasan, J. Malik, I. Bibi, W. Khan, F. Al-Wesabi, K. Dev, and G. Huang, "Securing industrial internet of things against botnet attacks using hybrid deep learning approach," *IEEE Transactions on Network Science and Engineering*, 2022.

[9] M. Cherian and S. Varma, "Mitigation of ddos and mitm attacks using belief based secure correlation approach in sdn-based iot networks," *International Journal of Computer Network & Information Security*, vol. 14, no. 1, 2022.

[10] B. Yakubu, M. Khan, A. Khan, F. Jabeen, and G. Jeon, "Blockchain- based ddos attack mitigation protocol for device-to-device interaction in smart home," *Digital Communications and Networks*, vol. 9, no. 2, pp. 383–392, 2023.

[11] Y. Kim, Y. Kim, and H. Kim, "Effective feature selection methods to detect iot ddos attack in 5g core network," *Sensors*, vol. 22, no. 10, p. 3819, 2022.

[12] J. Shroff, R. Walambe, S. Singh, and K. Kotecha, "Enhanced security against volumetric ddos attacks using adversarial machine learning," *Wireless Communications and Mobile Computing*, pp. 1–10, 2022.

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[13] S. Almeghlef, A. AL-Ghamdi, M. Ramzan, and M. Ragab, "Applica- tion layer-based denial-of-service attacks detection against iot-coap," *Electronics*, vol. 12, no. 12, p. 2563, 2023.
[14] B. Alabsi, M. Anbar, and S. Rihan, "Conditional tabular generative adversarial based intrusion detection system for detecting ddos and dos attacks on the internet of things networks," *Sensors*, vol. 23, no. 12, p. 5644, 2023.
[15] S. Rani, I. Ioannou, P. Nagaradjane, C. Christophorou, V. Vassiliou, S. Charan, S. Prakash, N. Parekh, and A. Pitsillides, "Detection of ddos attacks in d2d communications using machine learning approach," *Computer Communications*, vol. 198, pp. 32–51, 2023.
[16] W. Khedr, A. Gouda, and E. Mohamed, "Fmdadm: A multi-layer ddos attack detection and mitigation framework using machine learning for stateful sdn-based iot networks," *IEEE Access*, vol. 11, pp. 28 934– 28 954, 2023.
[17] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. Dhaou, "Distributed denial of service attack detection for the internet of things using hybrid deep learning model," *IEEE Access*, vol. 11, pp. 119 862– 119 875, 2023.
[18] H. Elubeyd and D. Yiltas-Kaplan, "Hybrid deep learning approach for automatic dos/ddos attacks detection in software-defined networks," *Applied Sciences*, vol. 13, no. 6, p. 3828, 2023.
[19] F. Sattari, A. Farooqi, Z. Qadir, B. Raza, H. Nazari, and M. Almutiry, "A hybrid deep learning approach for bottleneck detection in iot," *IEEE Access*, vol. 10, pp. 77 039–77 053, 2022.
[20] S. Yaras and M. Dener, "Iot-based intrusion detection system using new hybrid deep learning algorithm," *Electronics*, vol. 13, no. 6, p. 1053, 2024.
[21] M. Alzahrani and A. Bamhdi, "Hybrid deep-learning model to detect botnet attacks over internet of things environments," *Soft Computing*, vol. 26, no. 16, pp. 7721–7735, 2022.
[22] M. Ali, M. Jaber, S. Abd, A. Rehman, M. Awan, R. Damasˇevicˇius, and S. Bahaj, "Threat analysis and distributed denial of service (ddos) attack recognition in the internet of things (iot)," *Electronics*, vol. 11, no. 3, p. 494, 2022.
[23] R. Kumar, P. Kumar, R. Tripathi, G. Gupta, S. Garg, and M. Hassan, "A distributed intrusion detection system to detect ddos attacks in blockchain-enabled iot network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, 2022.
[24] V. Brindha Devi, N. Ranjan, and H. Sharma, "Iot attack detection and mitigation with optimized deep learning techniques," *Cybernetics and Systems*, pp. 1–27, 2022.
[25] S. Reddy and G. Shyam, "A machine learning based attack detection and mitigation using a secure saas framework," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4047–4061, 2022.
[26] Kaggle,"Ddos botnet attack on iot devices dataset," https://www.kaggle.com/datasets/siddharthm1698/ddos-botnet-attack-on-iot-devices/data, accessed: 2024-04-12.

Received: August 10, 2025