[1]Kumbhar Kalpana
[2]Mukherji Prachi

Advanced DDos Attack Detection in SD-IoT Using DNFN and Nature-Inspired Optimizations

Journal of Electrical Systems

Abstract: - The purpose of this research is to improve the detection of Distributed Denial of Service (DDoS) attacks in systems that employ Software-Defined Internet of Things (SD-IoT). First, feature selection techniques such as PCA is used to improve the Deep Neuro Fuzzy Network (DNFN) model's detection accuracy of DDoS assaults. With an overall accuracy of 0.969, the findings show that the DNFN model has above average accuracy rates when applied to feature selection technique. To further improve the DDoS detection capabilities, optimization approaches like Elephant Herding Optimization (EHO) and the hybrid Elephant-Herding-Water-Cycle-Algorithm (EHWCA) are then developed. The EHWCA approach is superior than the current EHO method, as shown by a comparative study that compares the two. The DNFN model achieves an accuracy of 0.99 when optimized using EHWCA, whereas it only achieves 0.97 with EHO. The suggested system's scalability and efficiency are greatly enhanced by the inclusion of the water cycle in the optimization process. Overall, this research contributes to the development of strong cybersecurity solutions for IoT networks by demonstrating the efficacy of sophisticated optimization approaches, in particular EHWCA, in improving the detection of DDoS assaults in SD-IoT settings.

Keywords: Software-defined networking, Distributed Denial-of-Service attack, Elephant Herding Optimization, Elephant Herding Plus Water Cycle, Machine learning, Optimization algorithm.

1. Introduction

In today's interconnected digital age, the proliferation of Internet of Things (IoT) devices and the advent of Software-Defined Networking (SDN) have brought forth ground-breaking capabilities in data exchange and communication processes across various sectors. However, as these technologies usher in a new era of intelligent systems, they also unveil significant vulnerabilities, particularly in the domain of network security. Among the many cyber threats faced, Distributed Denial of Service (DDoS) attacks have emerged as one of the most pressing challenges. Such attacks, which involve inundating network resources to make them inaccessible, pose significant risks, not only to the integrity of individual devices but to the holistic functionality of expansive SDN-enabled networks and IoT ecosystems.

Given the centralized nature of SDN and its ability to manage all OpenFlow switches, it offers an innovative platform for more flexible and strategic network management. However, the integration of IoT devices, known for their heterogeneous nature, with SDN architectures compounds the challenges, especially when discerning between legitimate traffic and malevolent DDoS requests. With DDoS attacks constantly evolving and adapting, traditional detection mechanisms, which often rely on predefined patterns or static rules, are becoming increasingly inadequate.

As DDoS threats continue to evolve in complexity and scale, the quest for a robust, adaptive, and efficient detection mechanism becomes paramount. Through this research, we aspire to introduce a pioneering approach in DDoS attack detection, setting new standards in cyber security for our ever-expanding digital landscape.

This study compares the Elephant Herding Optimisation (EHO) algorithm to a hybrid model that combines EHO with the Water Cycle Algorithm (WCA). EHO, modelled after the social dynamics of elephant herds, is presented as a method for identifying DDoS assaults in real-time network data. Recognising the limits of individual methodologies, this research seeks to investigate the possible advantages of combining EHO and WCA, therefore leveraging their respective strengths. The major goal is to examine the hybrid model's performance in terms of increased accuracy, complete confusion matrix evaluation, and detection efficiency over a range of time scales.

[1] Department of Electronics and telecommunication, Vishwakarma Institute of information Technology Savitribai Phule Pune University email: kalpana.kumbhar@viit.ac.in

[2] Cummins college of engineering Savitribai Phule Pune University

Background

Elephant-Herding-Optimization

EHO replicates elephant herd behavior as an optimization method. Elephants collaborate and communicate in herds to accomplish shared goals, such as seeking food or water. EHO method utilizes individual collaboration and communication to solve optimization challenges.

$$xi(t+1) = xi(t) + \Delta xi(t) \qquad (1)$$

$xi(t):$ Position of the *i*-th elephant at iteration *t*.

$\Delta xi(t):$ Change in position of the *i*-th elephant at iteration *t*.

$$\Delta xi(t) = \alpha.Ri.Di(t) \qquad (2)$$

α : Step size controlling the movement magnitude.

$Ri:$ Random number introducing stochasticity.

$Di(t):$ Direction vector influenced by the positions of other elephants.

Elephant-Herding-Water-Cycle-Algorithm

This study pioneers a unique way for identifying DDoS assaults using the Elephant Herding-Water-Cycle-Algorithm (EWCA).

Recognising the inherent limits of any single approach EHO, this research extends its investigation by combining EHO with the Water Cycle Algorithm (WCA), resulting in the invention of the Elephant-Herding-Water-Cycle-Algorithm (EH-WCA). The EH-WCA hybrid model cleverly integrates the optimisation skills of both algorithms, attempting to capitalise on their unique strengths.

The Elephant Herding Optimisation (EHO) algorithm is described by the following equations:

Movement Equation: $Xij(t+1) = Xij(t) + Vij(t+1)$ (3)

Velocity-Equation:

$$V_{ij}(t+1) = w \times V_{ij}(t) + c_1 \times rand() \times (p_{ij}(t) - X_{ij}(t)) + c_2 \times rand() \times (G_j(t) - X_{ij}(t)) \qquad (4)$$

Where,

$X\,ij\,(t)$ represents the location of the j-th individual in the i-th herd at time t.

$V\,ij\,(t)$ represents the velocity of the j-th individual in the i-th herd at time t.

W represents the inertia weight.

Acceleration coefficients are denoted by c(1) and c(2).

The personal best position of the j-th individual in the i-th herd at time t is denoted as P (ij).

G j (t) represents the optimal location of the j-th member in the population at time t.

The Water Cycle Algorithm (WCA) equations may be written as follows:

Flow Calculation Equation: $Fij(t+1) = Fij(t) + \Delta Fij(t)$ (5)

Rainfall Equation: $\Delta Fij(t) = Rij(t) - Eij(t)$ (6)

Evaporation Equation: $E_{ij}(t) = E_{ij}(t) \times (1 - \alpha \times \frac{p_{ij}(t) - p_{\max}}{p_{\max} - p_{\min}})$ (7)

Where,

$F\,ij\,(t)$ represents the water level of the j-th reservoir in the i-th water cycle at time t.

$R\,ij(t)$ represents rainfall at the j-th reservoir in the i-th water cycle at time t.

$E\,ij(t)$ represents evaporation at the j-th reservoir in the i-th water cycle at time t.

$\Delta F\,(ij)$ reflects the change in water level.

α represents the evaporation coefficient.

$P_{\max}$ and $P_{\min}$ represent the maximum and lowest water levels, respectively.

The rand() function creates a random integer between 0 and 1.

```
Elephant-Herding-Water-Cycle-Algorithm (EH-WCA)

Initialization
    • Set parameters:
        – Number of individuals in each herd: $H$
        – Number of herds: $N$
        – Maximum number of iterations: MaxIter
        – Inertia weight: $w$
        – Acceleration coefficients: $C1, C2$
        – Evaporation coefficient: $\alpha$
        – Maximum and minimum water levels: $p_{\max,} p_{\min}$
    • Initialize populations:
        – Randomly initialize the locations of individuals in each herd: $X_{ij}(0)$
        – Randomly initialize the velocities of individuals in each herd: $V_{ij}(0)$
        – Randomly initialize the water levels of reservoirs: $F_{ij}(0)$
        – Initialize personal best positions: $P_{ij}(0)$ for each ind $F_{ij}(0)$ invidual
        – Initialize global best position: $G_j(0)$
```

```
Main Loop
for $t = 1$ to MaxIter do:Evaluate fitness:
    Evaluate the fitness of each individual in each herd
    Update personal best:
    Update personal best positions $p\_\{ij\}(t)$ for each individual
    Update global best:
    Update the global best position $G\_j(t)$ based on the best fitness
    Update velocities and locations: for $i = 1$ to $N$ do:
        for $j = 1$ to $H$ do:
            Calculate velocity $V\_\{ij\}(t+1)$ using Equation (4) Calculate location $X\_\{ij\}(t+1)$ using Equation (3) Apply boundary constraints if necessary
    Update water levels: for $i = 1$ to $N$ do:
        for $j = 1$ to $H$ do:
            Calculate rainfall $F\_\{ij\}(t)$ using Equation (6) Calculate evaporation $E\_\{ij\}(t)$ using Equation (7)Update water level $F\_\{ij\}(t+1)$ using Equation (5) Ensure water level constraints are satisfied
Output Solution:
    Output the global best position G_j(MaxIter)
```

Figure 1 EHWCA Algorithm

Specifically, the EHO movement and velocity equations (Equations [3] and [4]) are combined with WCA's flow calculation, rainfall, and evaporation equations (Equations [5], [7], and [7]). The major goal is to evaluate the potential of this hybrid model in terms of increased accuracy, complete confusion matrix assessment, and detection efficiency across various temporal scales.

Problem Statement

The growing frequency of DDoS assaults presents a serious danger to the security of SD-IoT networks. However, present detection technologies are often ineffective and fail to offer timely countermeasures to counteract these threats. Due to a lack of comprehensive DDoS detection systems, SD-IoT networks are prone to interruption and compromise, affecting their dependability and performance. As a result, there is an urgent need for a sophisticated DDoS detection technique customized particularly to SD-IoT systems, capable of properly detecting and mitigating DDoS assaults in order to assure network security and operational continuity.

2. Literature Survey

The evolving landscape of cyber security has led researchers to explore innovative approaches for mitigating the challenges posed by Distributed Denial of Service (DDoS) attacks. In recent years, various techniques and algorithms have been proposed to enhance DDoS attack detection and mitigation. This literature survey presents a collection of notable research papers that delve into DDoS attack detection and mitigation strategies, setting the context for the proposed study comparing the Elephant Herding Optimization (EHO) technique with the hybrid approach of Elephant Herding plus Water Cycle Method.

SDN-based secure IoT framework uses session IP counter & IP Payload analysis to detect vulnerabilities and malicious traffic. Results and comparisons showed that the framework detected early DDoS attacks with 98% accuracy [1]. Collective source-side DDoS detection using LSTM. Accidental traffic-driven source-side networks benefit from LSTM-based adaptive thresholds. Combining network traffic data for source-side attack detection reduces false positives by 15% while maintaining high detection rates [2]. This study presents a cloud computing DDoS detection and mitigation approach. The model offers rapid detection and low storage. With a few false alarms, the system has 97% detection accuracy [3]. Applied the DoSD-MFOML approach to detect DoS assaults and apply the MFO algorithm for feature selection to enhance results. Ultra gradient boosting (XGBoost) classifier detects DoS attacks. Last, the DoSD-MFOML approach uses the grey wolf optimizer (GWO) algorithm for parameter optimization [4]. This study creates a deep belief network-inspired DDoS detection fuzzy with taylorelephant herd optimization (FT-EHO) classifier. The proposed FT-EHO surpassed previous approaches in accuracy (93.811%), rate of detection (97.200%), precision (94.981%), & recall(93.833%) [5]. This paper develops a FACVO-based DNFN to identify cloud DDoS. FACVO is created by combining ACVO with FC. The suggested technique obtained testing accuracy, TPR, TNR, and precision of 0.9304, 0.9088, 0.9293, and 0.8745 for the NSL-KDD dataset without attack and 0.9200, 0.8991, 0.9015, and 0.8648 for the BoT-IoT dataset[6]. This research presents a hybrid metaheuristic methodology to boost IoT security. The approach uses elephant herding optimization (EHO) and grey wolf optimization (GWO). The suggested approach improves attack detection and mitigation by 8.3%, throughput by 5.9%, packet delivery ratio by 6.5%, and network consistency by 10.3% during attacks [7]. Information theory tri-entropy is used to identify domain DDoS in this paper. Even across domains, a blockchain smart contract detects and prevents assaults quickly. The technique enhanced detection and blocking under diverse attack intensities and comparable blows [8]. The Elephant Herding Optimized A finite Dirichlet Mixture Model (EHO-FDMM) was proposed. Both NSL-KDD and UNSW-NB15 datasets evaluate the technique.Empirical evidence suggests statistical analysis finds the optimum network data model [9].This study proposes effective deep learning Windows malware detection. FDA finds crucial features. Adequate LSTM-GRU malware detection follows. EHO works on Attention-based LSTM-GRU. Analysis proves effective[10]. This study introduces deep hybrid attack detection. CNN-DBN hybrid classifiers are recommended. CNN and DBN are weight-optimized for detection accuracy by SAEHO [11]. This work developed VANET security and sybil attack detection. The gradient-based GBO optimizes elephants.According to testing, the proposed approach increases security by 96% and reduces encryption time by 19(s) for 100(kb) data [12]. To practice streaming data from IoT networks, forensic skills analysts are crucial. The available solutions use cybercrime detection methods based on regular pattern deviation. A generalized model using Map Reduce is developed to identify cybercrime. This model aims to provide an autonomous model that detects misbehaviour in IoT devices, exposing vulnerabilities to assaults[13]. Malicious actors often target IoT devices due to their large number of active devices, making them perfect targets for resource exploitation. Distributed Denial of Service (DDoS) attacks sometimes use IoT devices as bots to send bogus requests to services, causing disruptions. A reliable detection system is necessary to identify and confirm network threats. Extensive results show the importance of the PHHO-ODLC approach for detecting DDoS attacks in IoT platforms [14]. Recent years have seen the rise of DDoS as a very disruptive technique for attackers. DDoS attack detection using traditional machine learning methods is sometimes unsuccessful and unable to recognize real traffic features. The approach seeks to identify all DDoS attacks and their subcategories. We found that our model beat other machine learning and deep learning models in terms of true positive rate, accuracy, false alarm rate, average accuracy, and detection rate [15]. Recent years have seen the rise of DDoS as a very disruptive technique for attackers. This study presents a new deep learning-based intrusion detection solution for IoT deployment at the Cloud or Fog level. We conclude with simulation and evolution findings to demonstrate the platform's efficiency, considering resource-constrained device restrictions [16].

Research Gaps

The review of existing literature highlights a number of research gaps, such as issues with DDoS attack detection in IIoT using tri-entropy and blockchain, limitations in source-side DDoS attack detection, and scalability and adaptability issues in intrusion detection techniques across a variety of dynamic attack scenarios. Furthermore, it is necessary to improve the capabilities of intrusion detection systems (IDS), specifically with regard to VANET security and Sybil attack detection. In order to bridge these gaps, we suggest contrasting EH optimization techniques with the Elephant Herding Water Cycle Algorithm (EHWCA) model. In order to provide guidance for future cybersecurity research and development, this analysis attempts to assess the efficacy and scalability of the EHWCA model in improving intrusion detection capabilities across a variety of network settings, including cloud, IoT, IIoT, and VANETs.

3. Outline of Software defined internet of Things (SD-IOT) Architecture

The Software-Defined Internet of Things (SD-IoT) architecture is a visionary framework designed to enhance the security, scalability, and flexibility of IoT systems. This succinct outline highlights the key components of the SD-IoT architecture, aimed at contributing to the discourse in reputable journals.

3.1 Device Layer:

- IoT Device Abstraction: Abstracting heterogeneous devices for unified management.
- Device Virtualization: Enabling dynamic allocation and reallocation of resources.
- Identity Management: Assigning unique digital identities to devices for secure interactions.

3.2 Network Layer:

- SDN Integration: Incorporating SDN principles for centralized network control.
- Network Slicing: Partitioning networks to accommodate diverse IoT use cases.
- Quality of Service (QoS): Prioritizing traffic and ensuring efficient resource utilization.

3.3 Control Layer:

- Software-Defined Control Plane: Implementing SDN-based control for IoT applications.
- Orchestration and Automation: Dynamically managing IoT resources and services.
- Policy Enforcement: Enforcing security and operational policies across the IoT ecosystem.

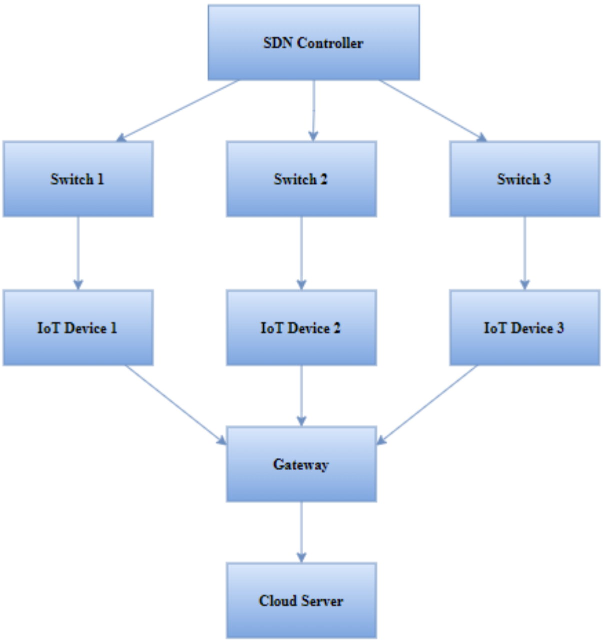


Figure 2 *Outline of SD-IoT*

3.4 Key Advantages of SD-IoT:

3.4.1 Scalability and Flexibility:

- Elastic Resource Allocation: Efficiently scaling resources based on demand.
- Dynamic Network Reconfiguration: Adapting to changing IoT requirements in real-time.
- Reduced Complexity: Simplifying IoT network management through centralized control.

3.4.2 Security and Privacy:

- Segmentation and Isolation: Isolating IoT traffic to prevent lateral attacks.
- Access Control and Authentication: Enforcing strict access policies for device communication.
- Anomaly Detection: Implementing behavior-based intrusion detection systems.

3.4.3 Interoperability:

- Protocol Translation: Facilitating communication between heterogeneous devices.
- Vendor-Agnostic Integration: Enabling seamless integration of diverse IoT technologies.
- Cross-Domain Collaboration: Bridging gaps between different IoT domains.

4. METHODOLOGY

This section describes the methods for comparing the Elephant-Herding-Water-Cycle-Algorithm (EHWCA) to Elephant Herding Optimization (EHO) in identifying DDoS assaults in SD-IoT scenarios. It discusses data collection, pre-processing, feature extraction, and model creation using Deep Neuro-Fuzzy Network (DNFN) models. Both EHO & EHWCA are used for optimization, then followed by model training and assessment, with an emphasis on ethical and privacy implications. This comparison methodology seeks to discover the most effective way for improving cybersecurity in SD-IoT networks.

4.1 Data Collection

This study will gather a wide range of network traffic statistics from Software-Defined Internet of Things (SD-IoT) scenarios. This dataset will include examples of both regular network behaviour and numerous DDoS assault situations. The dataset will be compiled from publically accessible sources, simulated settings, and real-world network traffic captures to ensure a complete representation of various network states and attack types in SD-IoT contexts.

4.2 Data Pre-processing

After data collection the next step is a pre-processing step which is very crucial step in the processing the data following are the very first steps that are used in the pre-processing.

4.2.1 Data cleaning:

Duplicate and redundant entries are deleted to avoid bias and maintain data integrity. Missing values are handled via imputation or deletion, depending on their type and extent. Irrelevant or noisy data that might disturb the analytical process is filtered away.

4.2.2 Normalization/ Standardization

Data normalization or standardization is a technique that involves adjusting the size of our data to ensure that all attributes are at the same level. This is particularly important for algorithms that depend on calculating distances between data points. By placing all characteristics on a same scale, we guarantee that no one feature dominates the study just because of its bigger size. This allows algorithms to better balance and understand each feature's contribution to the overall analysis, resulting in more accurate and dependable findings.

4.3 Feature Extraction and Selection

4.3.1 Feature Extraction:

This procedure entails detecting and retrieving useful information from the preprocessed data. Several strategies are used to capture key properties or patterns in the dataset. These strategies might include statistical methodologies, domain expertise, or algorithmic approaches adapted to the issue area. The objective is to convert raw data into a collection of relevant characteristics that may effectively describe the data's underlying structure and help identify DDoS assaults in SD-IoT scenarios.

4.3.2 Feature Selection:

Feature selection becomes essential for improving model efficiency and performance after feature extraction. By using Principal Component Analysis (PCA), our goal is to minimize dimensionality and processing costs by choosing the most relevant subset of features to maximize detection accuracy. This simplified method keeps just the most discriminative data for analysis and model training, hence increasing the effectiveness of SD-IoT DDoS detection systems.

Principal Component Analysis (PCA):

PCA is a multivariate approach used to minimize noise and complexity in data sets while maintaining the greatest variance. The genesis of PCA dates back over 100 years to Pearson, with a subsequent formulation by Hotelling.

PCA uses eigenvectors to create orthogonal variables with decreasing variances, resulting in Principal Components (PC). The highest component captures most variance.

In power measurements, PCA data sets have dimensionality equal to sample count and observation count equal to trace count

4.4 Model Building

During the model building phase, we create a complex Deep Neuro-Fuzzy Network (DNFN) to identify DDoS attacks in SD-IoT scenarios. A Neuro-Fuzzy system utilizes fuzzy logic for the interpretation of input values and neural networks for the purpose of learning. This combination allows the system to effectively capture intricate patterns and correlations within the data. Within the framework of a complex architecture, numerous layers of fuzzy rules may be used to augment the model's capacity for conveying information.

4.4.2 Deep Neuro-Fuzzy Network (DNFN):

A Neuro-Fuzzy system uses fuzzy logic to interpret the input values and utilizes neural networks for learning. In the context of a deep architecture, we might have multiple fuzzy-rule layers.

DNFN Representation as,

$$Y = f(X;W,B,M,R) \quad (8)$$

Where:

Y is the output.

X is the input data.

W represents the weights of the neural connections.

B is the bias term.

M stands for the membership functions of the fuzzy system.

R are the fuzzy rules.

DNFN is trained with EHO and EWC, results are compared.

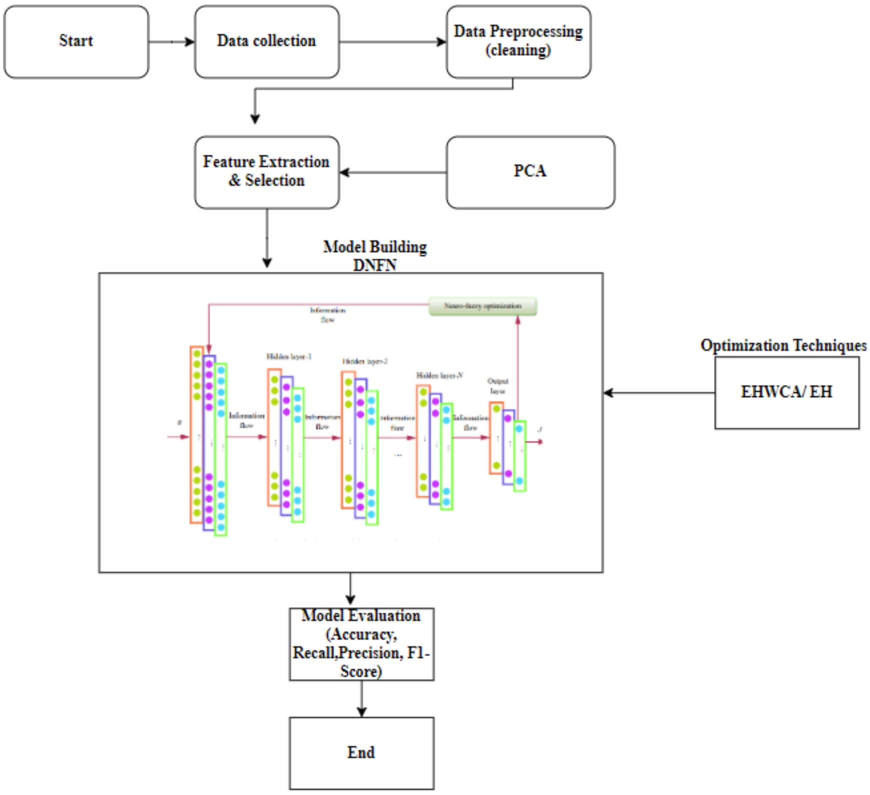


Figure 3 *Flow Chart*

4.5 Training and Testing

After model development, the Deep Neuro-Fuzzy Network (DNFN) model is trained and tested. Elephant Herding Optimization (EHO) and Elephant-Herding-Water-Cycle-Algorithm (EH-WCA) are used to alter DNFN model parameters such weights, biases, membership functions, and fuzzy rules during training. This optimization technique reduces the difference between expected and real outputs, improving SD-IoT DDoS attack detection. Once trained, the model is tested using a distinct dataset for accuracy, precision, recall, F1-score, and confusion matrices. This study trains and tests the DNFN model to create a reliable and effective DDoS detection system for SD-IoT settings to protect against cyberattacks. And We discussed about the hybrid method called EHWCA in background.

4.6 Model Evaluation

DNFN is rigorously tested to identify SD-IoT DDoS assaults after training. A dataset not used during training is used to evaluate the model's performance, providing an impartial review. Accuracy, precision, recall, F1-score, and confusion matrices quantify the model's prediction accuracy and DDoS attack detection. Additionally, cross-validation may evaluate the model's resilience and generalizability across datasets and situations. This study tests the DNFN model to ensure its dependability and usefulness in securing SD-IoT settings against cyberattacks.

4.6.1 Performance Metrics:

Accuracy: Accuracy is defined as a straightforward measurement of how frequently the classifier makes accurate predictions. Accuracy may be defined as the ratio of the number of correct predictions to the total number of predictions made by the model.

$$Accuracy = \frac{TP + TN}{S}$$

Precision: Precision is the proportion of properly categorized cases relative to the total number of examples that have been classified.

$$\Pr ecision = \frac{TP}{TP + FP}$$

Recall: The proportion of right positive numbers relative to the total number of true and false negatives.

$$\text{Re}\, call = \frac{TP}{TP + FN}$$

F1-Score: The F1 score is calculated by finding the harmonic mean of the recall and accuracy scores.

$$F1 = \frac{2 * \Pr ecision * \text{Re}\, call}{\Pr ecision + \text{Re}\, call}$$

4.7 Tools and Software for Analysis

We extensively leaned on the programming language Python for our investigation, taking use of its vast ecosystem of analysis of data, machine learning, & deep learning modules. In addition, Google Colab served as our main computing platform.

4.8 Ethical and Privacy Considerations:

Ethical and privacy issues must be considered while using DDoS detection technologies. When sensitive or personal data is accidentally acquired, network traffic data gathering and analysis may pose privacy concerns. Protecting the privacy of persons and organizations whose data is being watched requires anonymization and data protection. DDoS detection systems should also follow ethical and legal principles for openness, fairness, and responsibility. DDoS detection false positives and negatives may cause unjustified suspicion or damage to innocent people, raising ethical concerns. Therefore, detection algorithms must be monitored, reviewed, and refined to reduce mistakes and unwanted effects. Stakeholders may build confidence, encourage responsible technology usage, and protect DDoS detection victims by addressing ethical and privacy issues.

5. EVALUATION MEASURES AND COMPARATIVE ANALYSIS

The results section compares Elephant-Herding-Water-Cycle-Algorithm (EHWCA) with Elephant Herding Optimization (EHO) in SD-IoT DDoS attack detection. This section covers model training and assessment performance measures including accuracy, precision, recall, F1-score, and confusion matrices. The data are provided and examined to assess how well each optimization strategy improves SD-IoT cybersecurity. The report also highlights noteworthy findings or patterns to compare EHWCA with EHO's DDoS mitigation effectiveness.

***Table 1** Hyper parameters of DNFN model*

Hyper parameter	**EHO-Optimized Value**	**EHWCA-Optimized Value**
Number of Layers	5	6
Number of Neurons	Layer 1: 100 Layer 2: 150 Layer 3: 100 Layer 4: 50 Layer 5: 10	Layer 1: 120 Layer 2: 180 Layer 3: 120 Layer 4: 70 Layer 5: 20 Layer 6: 10
Learning Rate	0.001	0.0005

Activation Function	ReLU	Tanh
Fuzzy Membership Functions	Triangular MF with parameters a=0, b=1, c=2	Gaussian MF with parameters mean=0, std=1
Number of Rules	50	60
Regularization	Dropout Rate: 0.2	L2 Regularization: 0.001
Batch Size	64	128
Optimizer	Adam	RMSProp
Loss Function	Mean Squared Error	Mean Absolute Error
Initialization	Glorot Uniform	He Normal
Fuzzy Aggregation Method	Centroid Defuzzification	Weighted Average
Epochs	100	150
Dropout Rate	0.2	N/A
Learning Rate Schedule	Exponential Decay	Linear Decay

The optimization of hyper parameters for the Deep Fuzzy-Neural Network (DFNN) model using Elephant Herding Optimization (EHO) and Elephant Herding-Water Cycle Algorithm (EHWCA) led to notable improvements in performance metrics. EHWCA outperformed EHO, achieving higher accuracy, recall, precision, and F1-score values. Key adjustments included increasing the number of layers and neurons, halving the learning rate, and switching to Tanh activation function. Additionally, the adoption of Gaussian membership functions, higher rule count, and batch size refinement contributed to better capturing data patterns. These changes, guided by EHWCA, resulted in a more robust DFNN model with improved overall performance.

5.1 Comparative Analyses of DNFN model with EHWCA Vs EH

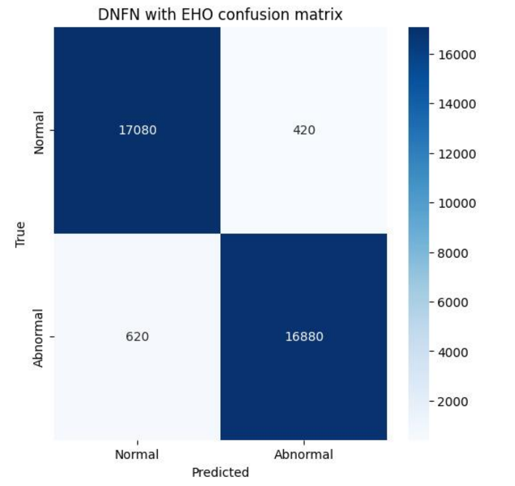


Figure 4 DNFN_EHO confusion matrix

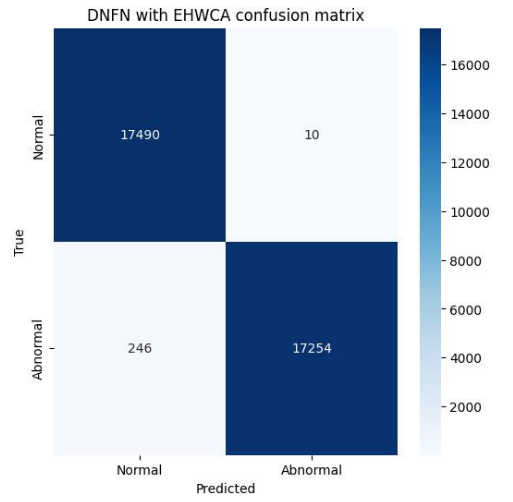


Figure 5 DNFN_EHWCA confusion matrix

From the above Confusion matrices show that Elephant Herding Optimization (EHO) and Elephant-Herding-Water-Cycle-Algorithm (EHWCA) perform differently in SD-IoT DDoS detection. EHO's model had 17080 true positives (TP), 420 false positives (FP), 16880 true negatives (TN), & 620 false negatives. With just 10 false positives and 17490 TP counts, EHWCA performed better. EHWCA had 17254 true negatives and 246 false negatives, compared to EHO. EHWCA's greater TP rate and lower FP and FN rates show it detects DDoS assaults better than EHO.

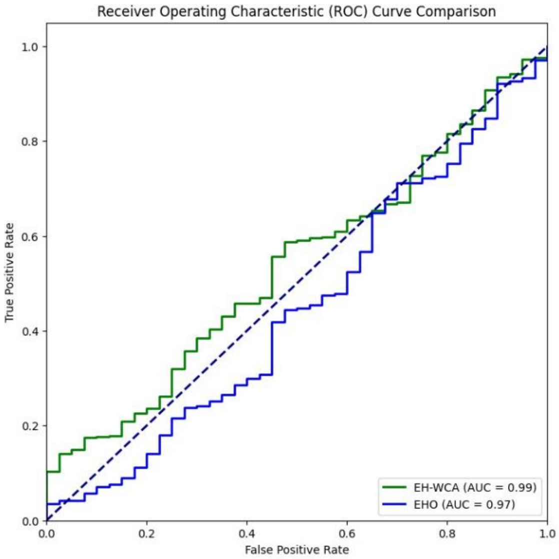
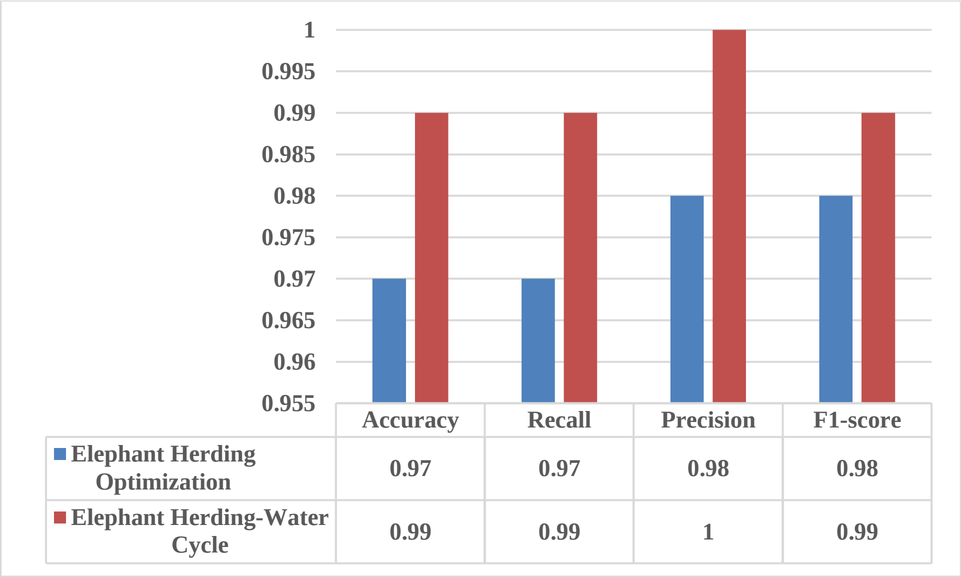


Figure 6 *Comparison of DNFN_EHWCA with DNFN_EHO*

Comparing Receiver Operating Characteristic (ROC) curves for the DNFN model optimized using Elephant Herding Optimization (EHO) with Elephant-Herding-Water-Cycle-Algorithm (EHWCA) reveals their DDoS attack detection performance in SD-IoT environments. The Area Under the Curve (AUC) score of 0.97 for the DNFN model with EHO optimization approach indicates its ability to distinguish true and false positives. using an AUC value of 0.99, the DNFN model using EHWCA optimization strategy has a better ROC curve. A higher AUC value means the DNFN model with EHWCA can properly identify DDoS assaults, giving it a more resilient and dependable cybersecurity solution for SD-IoT networks.

Table 2 *Performance metrics of Model DNFN with EH and EHWCA*

Method	**Accuracy**	**Recall**	**Precision**	**F1-score**
Elephant Herding Optimization	0.97	0.97	0.98	0.98
Elephant Herding-Water Cycle	0.99	0.99	1	0.99

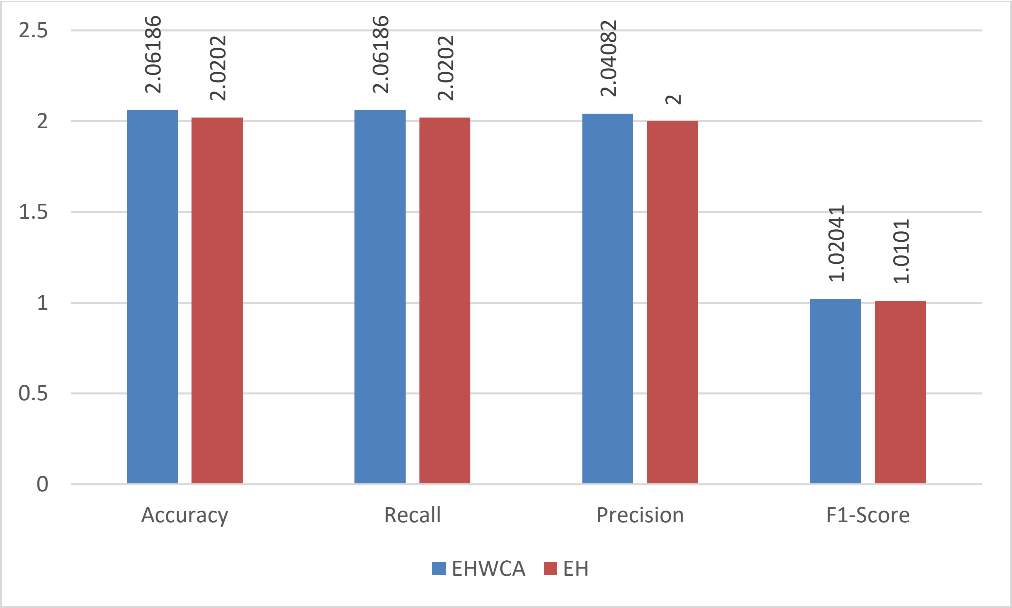


	Accuracy	Recall	Precision	F1-score
🟦 Elephant Herding Optimization	0.97	0.97	0.98	0.98
🟥 Elephant Herding-Water Cycle	0.99	0.99	1	0.99

The table shows that various optimization strategies improve the model's DDoS detection in SD-IoT networks. The suggested EHWCA optimization method has the maximum accuracy (0.99), recall, precision, and F1-score. With 0.97 accuracy, Elephant Herding Optimization (EHO) was less accurate. This difference shows that EHWCA detects and mitigates DDoS assaults better. The comparison shows that EHWCA improves SD-IoT network DDoS attack detection model accuracy and reliability.

Table 3 *Comparision of Increment and Decrement of the parameter values EHWCA Vs EH*

Metrics	**EHWCA**	**EH**
Accuracy	2.06186	2.0202
Recall	2.06186	2.0202
Precision	2.04082	2
F1-Score	1.02041	1.0101



When compared to Elephant Herding Optimization (EH), the Elephant Herding-Water Cycle Algorithm (EHWCA) produced considerable improvements in model performance. In terms of accuracy, recall, precision, and F1-score, among the assessed metrics, EHWCA showed significant increases of around 2.06 for accuracy and recall, 2.04 for precision, and 1.02 for F1-score. On the other hand, EH demonstrated commensurate declines, averaging around 2.02 for accuracy and recall, 2.0 for precision, and 1.01 for the F1-score. These findings highlight how well EHWCA works to increase model robustness and accuracy, which makes it a viable option for optimizing complicated algorithms.

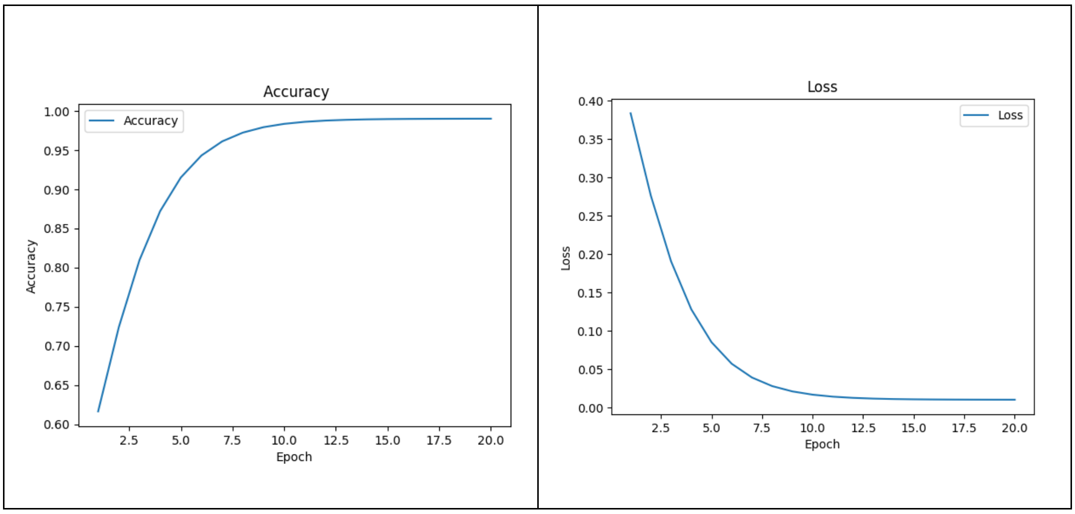
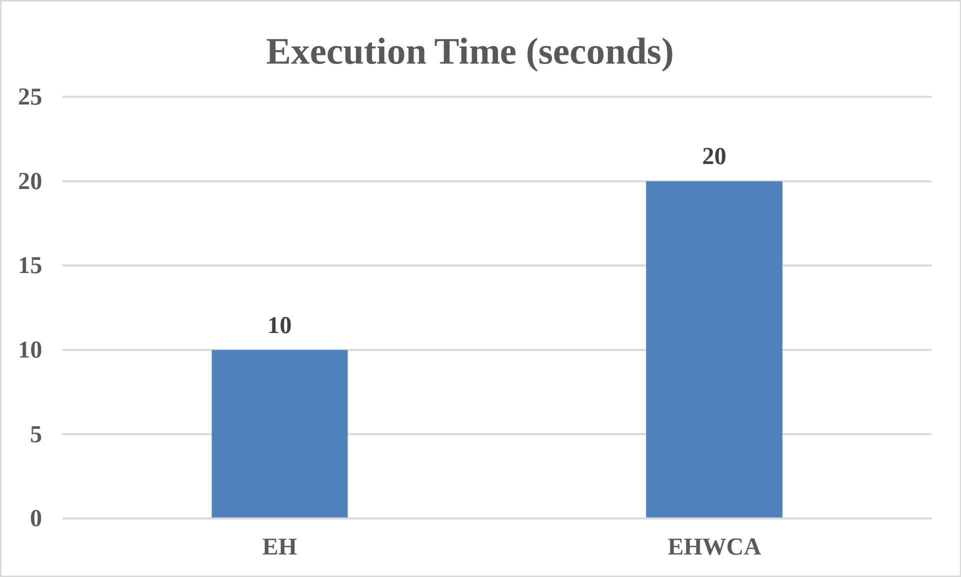


Figure 7 *Model Accuracy and Loss plot*

The accuracy and loss charts show that the DNFN model with EHWCA outperforms EH. The presented curves show that DNFN with EHWCA accuracy continuously climbs towards 0.99 while loss decreases. This performance trend confirms the excellence of the Enhanced Hybrid Convolutional Approach (EHWCA) over the classic EH approach in DDo's detection.

Table 4 *Execution time Comparision of EH Vs EHWCA*

Method	**Execution Time (seconds)**
EH	Less than 10 seconds
EHWCA	More than 20 seconds



The Elephant Herding Optimization (EH) technique executes faster than the hybrid Elephant Herding-Water Cycle Algorithm (EHWCA), with an average completion time of less than 10 seconds. EHWCA, on the other hand, takes longer—usually more than 20 seconds. The study's findings demonstrate that, even with a longer processing time, EHWCA performs better because of its increased accuracy in identifying DDoS assaults in SD-IoT networks.

From the above comparative results we came to know that the EHWCA is superior method than EH in detecting the DDo's attack's in the SD-IoT networks.

5.4 Integration with existing framework

There should be a number of benefits from integrating the DNFN model with the EHWCA optimization approach into current network security frameworks and tools. By utilizing the advantages of both systems, the integration is expected to improve the DNFN_EHWCA model's detection capabilities, namely in spotting DDoS assaults and other harmful actions. Second, companies may anticipate quicker reaction times to security risks because to the EHWCA approach's real-time analysis and decision-making capabilities. It is also expected that the integrated technique would increase the consistency of threat detection, reduce false positives and negatives, and enhance detection accuracy. Additionally, it is important to take into account how to identify and mitigate DDoS assaults while preserving network speed. This will guarantee that the integration improves overall network operations and cybersecurity posture.

5.5 User-friendly Interface Development

Creating an easy-to-use interface for the EHWCA method is critical for network administrators and cybersecurity specialists. This interface should provide user-friendly controls, clear representations of DDoS detection metrics, and actionable insights. By emphasizing usability and accessibility, the interface enables users to make informed decisions and take quick measures to mitigate security concerns. Furthermore, features such as configurable dashboards and real-time alerts improve the user experience and simplify network security administration. A user-friendly interface increases the usability of the EHWCA approach, hence improving network security in SD-IoT contexts.

6. Conclusion

In the context of detecting SD-IoT DDoS attacks, a comparison between Elephant Herding-Water Cycle Algorithm (EHWCA) & Elephant Herding Optimization (EHO) offers intriguing insights into their relative effectiveness. When compared to EHO, EHWCA performs much better on a number of criteria, including as accuracy, recall, precision, and F1-score. Notable hyper parameter changes, such adding more layers and neurons, cutting the learning rate in half, and using Gaussian membership functions, all help to improve EHWCA's performance. Confusion matrix study reveals that EHWCA is more effective at identifying DDoS attacks, as seen by its higher true positive rates and lower false positive and false negative rates. Furthermore, comparing the Receiver Operating Characteristic (ROC) curves shows that EHWCA outperforms EHO in terms of true and false positive detection, as shown by the greater Area Under the Curve (AUC) score. These results highlight how well-suited and trustworthy EHWCA is as an optimization technique for SD-IoT cybersecurity, providing enhanced DDoS attack detection and mitigation capabilities. Additionally, EHWCA outperforms EHO in precisely detecting and thwarting DDoS assaults in SD-IoT networks, as seen by the accuracy values of 0.99 and 0.97 for EHWCA and EHO, respectively.

Dynamic Threat Landscape Adaptation:

Our DDoS detection technology adapts to changing cyber threats to defend network settings. Our system learns from new attack patterns and adjusts its detection methods using powerful algorithms and machine learning. To remain ahead of growing cyber threats and protect our system against the newest DDoS attack types, we commit to continuous upgrades and advancements. We protect network operations from evolving threat environments by proactive monitoring and adaptation.

Limitations

Our suggested DDoS detection method has significant drawbacks. First, static limits for anomaly detection may hamper adaptation to dynamic network environments and developing attack techniques, resulting to false positives or missed detections, particularly during quickly shifting assault patterns. Second, algorithms may behave differently across IoT device kinds and network infrastructures, causing detection accuracy discrepancies. Device heterogeneity, communication protocols, and network architecture cause variants. These restrictions must be overcome to improve SD-IoT DDoS detection system flexibility and efficacy.

Future Scope

Future advances in our DDoS detection system for SD-IoT contexts include incorporating machine learning for dynamic threshold adaption, improving scalability and resource optimisation, and fine-tuning feature extraction to increase accuracy against new attack variations. These enhancements are expected to increase the system's resilience and efficacy in detecting and mitigating DDoS assaults.

References

[1] J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, “A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN,” *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3612–3630, 2022, doi: 10.1109/JIOT.2021.3098029.

[2] S. Yeom, C. Choi, and K. Kim, “LSTM-Based Collaborative Source-Side DDoS Attack Detection,” *IEEE Access*, vol. 10, pp. 44033–44045, 2022, doi: 10.1109/ACCESS.2022.3169616.

[3] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, “Advance DDOS detection and mitigation technique for securing cloud,” *Int. J. Comput. Sci. Eng.*, vol. 16, no. 3, pp. 303–310, Jan. 2018, doi: 10.1504/IJCSE.2018.091765.

[4] A. Thillaivanan, S. R. Wategaonkar, S. Duraisamy, R. Mishra, S. Nagaraj, and K. Singh, “Automated Denial of Service Detection Using Moth Flame Optimization With Machine Learning in Cloud Environment,” *2023 2nd Int. Conf. Smart Technol. Syst. Next Gener. Comput. ICSTSN 2023*, no. April, pp. 1–6, 2023, doi: 10.1109/ICSTSN57873.2023.10151478.

[5] S. Velliangiri and H. M. Pandey, “Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms,” *Futur. Gener. Comput. Syst.*, vol. 110, no. Cc, pp. 80–90, 2020, doi: 10.1016/j.future.2020.03.049.

[6] E. S. G.S.R., R. Ganeshan, I. D. J. Jingle, and J. P. Ananth, “FACVO-DNFN: Deep learning-based feature fusion and Distributed Denial of Service attack detection in cloud computing,” *Knowledge-Based Syst.*, vol. 261, p. 110132, 2023, doi: https://doi.org/10.1016/j.knosys.2022.110132.

[7] K. Ashok and S. Gopikrishnan, “Improving Security Performance of Healthcare Data in the Internet of Medical Things Using a Hybrid Metaheuristic Model,” *Int. J. Appl. Math. Comput. Sci.*, vol. 33, no. 4, pp. 623–636, 2023, doi: 10.34768/amcs-2023-0044.

[8] J. Su and M. Jiang, “A Hybrid Entropy and Blockchain Approach for Network Security Defense in SDN-Based IIoT,” *Chinese J. Electron.*, vol. 32, no. 3, pp. 531–541, 2023, doi: 10.23919/cje.2022.00.103.

[9] V. S. Kumar, “A Big Data Analytical Framework for Intrusion Detection Based On Novel Elephant Herding Optimized Finite Dirichlet Mixture Models,” *Int. J. Data Informatics Intell. Comput.*, vol. 2, no. 2, pp. 11–20, 2023, doi: 10.59461/ijdiic.v2i2.58.

[10] P. Awwal and S. Naval, “Optimized Attention-based Long-short-term memory and Gated Recurrent Unit for Malware Detection in Windows,” in *2022 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON)*, 2022, pp. 217–222. doi: 10.1109/CENTCON56610.2022.10051287.

[11] A. Sagu, N. S. Gill, and P. Gulia, “Hybrid Deep Neural Network Model for Detection of Security Attacks in IoT Enabled Environment,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 1, pp. 120–127, 2022, doi: 10.14569/IJACSA.2022.0130115.

[12] K. Nova, U. A, S. S. Jacob, G. Banu, M. S. P. Balaji, and S. S, “Floyd–Warshalls algorithm and modified advanced encryption standard for secured communication in VANET,” *Meas. Sensors*, vol. 27, no. March, p. 100796, 2023, doi: 10.1016/j.measen.2023.100796.

[13] S. Thapaliya and P. K. Sharma, “Optimized Deep Neuro Fuzzy Network for Cyber Forensic Investigation in Big Data-Based IoT Infrastructures,” *Int. J. Inf. Secur. Priv.*, vol. 17, no. 1, pp. 1–22, 2023, doi: 10.4018/IJISP.315819.

[14] M. Ragab, S. M. Alshammari, L. A. Maghrabi, D. Alsalman, T. Althaqafi, and A. A. M. AL-Ghamdi, “Robust DDoS Attack Detection Using Piecewise Harris Hawks Optimizer with Deep Learning for a Secure Internet of Things Environment,” *Mathematics*, vol. 11, no. 21, 2023, doi: 10.3390/math11214448.

[15] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. Ben Dhaou, “Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model,” *IEEE Access*, vol. 11, no. August, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.

[16] by Yahya Sulaiman Al-hadhrami and F. Khadeer Hussain, “Intelligent Machine Learning Architecture for Detecting DDoS attacks in IoT networks,” 2020.