10.48047/jocaaa.2024.33.02.25

A Scalable Deep Learning-Metaheuristic Approach for DDoS Attack Mitigation

[1]Mrs. Manjula HT, Research scholar, Department Of ISE, Atria Institute Of Technology, Bangalore
[2]Dr. Jyoti Metan, Associate Professor Department Of ISE, Atria Institute Of Technology, Bangalore

Abstract

Distributed denial-of-service (DDoS) attacks, which inundate targeted systems with traffic from several sources, pose a significant threat to computer networks and systems. Detecting these attacks in real-time has become a crucial responsibility in cybersecurity. Current methodologies for identifying DDoS assaults struggle to discern the complex patterns of attack traffic and exhibit a significant false positive rate. This study presents an improved methodology for identifying DDoS attacks with an Optimized Cybernet Model (OpCyNet), a deep learning framework combined with the Developed Battle Royale Optimization Algorithm (DBRA), utilizing the CICDDoS2019 dataset. The OpCyNet model comprises eleven learnable layers designed to extract, enhance, and classify attributes of network data. The architecture comprises three fully linked layers and eight convolutional layers. To enhance generalization and mitigate overfitting, the model employs dropout layers, max-pooling, batch normalization, leaky ReLU activation, among other techniques. Furthermore, cross-channel normalization and softmax classification augment the model's capacity to differentiate between normal and malicious network traffic patterns. The DBRA metaheuristic algorithm optimizes feature selection and classification, significantly decreasing computing costs while maintaining excellent detection accuracy. Experimental findings on the CICDDoS2019 dataset indicate that the OpCyNet-DBRA model surpasses traditional deep learning and machine learning methods regarding accuracy, precision, recall, F1-score, and false positive rate (FPR). The proposed architecture enhances threat detection and mitigation in real-world network environments, demonstrating efficiency, scalability, and intelligence. This work presents a method for cyberattack detection that integrates deep learning with metaheuristics to bolster cybersecurity resilience against evolving distributed denial-of-service (DDoS) attacks. Future efforts will focus on enhancing the proposed system's efficacy through real-time implementation, resilience against adversarial attacks, and validation across diverse datasets.

10.48047/jocaaa.2024.33.02.25

Keywords: Distributed denial-of-service; Developed Battle Royale Optimization Algorithm; Optimized Cybernet Model; Cross-channel normalization; Cybersecurity resilience.

1. **Introduction**

The Smart Micro-Grid (SMG) represents a cutting-edge model within the Modern Power Grid, utilizing information and communication technologies (ICTs) such as artificial intelligence, blockchain, game theory, and Internet-of-Things frameworks to ensure reliable energy service and prompt, robust interaction among all components. It is anticipated that SMG will possess the adaptability and intelligence to identify, locate, and address problems such as power outages resulting from terrorist activities, cyberattacks, or natural disasters. Machine learning (ML) represents a transformative development in artificial intelligence (AI) that empowers computers to learn to process inputs and outputs in a defined manner, so facilitating predictions and recommendations in SMG [4]. This is achieved by assessing and analyzing the supplied historical data rather than uncritically adhering to programming instructions. Mathematical models that depend significantly on matrix operations and linear algebra require extensive historical data and increased flexibility in parameter adjustments to improve the learning system's performance, particularly concerning accuracy and precision [5-6]. For instance, to enhance the reliability of the learning system, deep learning (DL) and artificial neural networks (ANN) may necessitate billions of weights in each layer [7]. The rapid advancement of smart city applications presents a considerable risk to traditional encryption, as its security relies on assumptions regarding computational complexity. In a metaverse application for a modern power grid, individuals' transitions between the physical and virtual realms complicate the prediction of their identity and privacy. SMG's performance is very contingent upon the available computational hardware and other processing capabilities because to its dependence on ML models.

With the increasing frequency and complexity of attacks on cloud computing, the necessity for enhanced measures to protect sensitive information and maintain system integrity has become paramount [9]. Several intrusion detection systems are now being developed to counter these attacks through the application of machine learning techniques. DDoS attacks represent a substantial threat and can inflict considerable harm on systems, especially those functioning in the cloud [10, 11]. A significant number of individuals lose confidence in the service, resulting in substantial financial losses for enterprises. Cloud computing infrastructures provided by

10.48047/jocaaa.2024.33.02.25

government agencies, educational institutions, financial institutions, and other public and private organizations must be sufficiently and consistently safeguarded against threats [12–13]. These companies have long ensured their security with an exclusive network design. Organizations safeguard their networks by deploying firewall technologies and employing specialists in the domain. The expenses related to hosting, maintaining, and safeguarding an institution's information systems and infrastructures are substantial in contemporary times [14–15]. Cloud computing services are progressively being delegated to centralized providers such as Amazon Web Services (AWS), Google Cloud, and Microsoft Azure, which function from multiple data centers worldwide. Ensuring security for these cloud systems is now more critical than ever due to their centralized architecture. This has resulted in numerous diverse methods to ensure security [16].

The objective of this paper is to develop a Deep Learning-based system capable of properly and reliably identifying various types of DDoS attacks while reducing false-positive rates [17]. Furthermore, the study's balanced sub-datasets were derived from the commonly utilized CIC-DDoS2019. Consequently, the redundant data was eliminated, and the attributes with minimal impact on the detection system were identified prior to the random sampling of each assault type. The leading deep learning model was recognized for its accuracy and inference performance. Two separate subsets of a randomly sampled dataset were acquired, and their influence on performance was examined in the study using min-max and logarithmic normalization methods. A variety of machine learning methodologies are employed for distributed denial of service attacks, as indicated by a review of the literature. Deep learning models rank among the most used methodologies in this domain. Researchers commonly derived sub-datasets by randomly partitioning the extensive CIC-DDoS2019 dataset. The data sets obtained after feature selection generally did not consider redundant samples, as indicated by the analysis of research performed on this dataset. Thus, use same samples for both training and testing yields exceptional outcomes. The subsequent statement delineates the principal aim of the work:

1. To construct the OpCyNet deep learning model, incorporating several convolutional layers, activation functions, and fully linked layers for effective feature extraction and classification of network attacks.

10.48047/jocaaa.2024.33.02.25

2. To optimize the parameters and enhance classification performance with the Developed Battle Royale Optimization Algorithm (DBRA), hence reducing computing complexity while increasing detection accuracy.

3.To assess the proposed model using the CICDDoS2019 dataset, confirming its capability to accurately identify and mitigate DDoS assaults with high precision and minimal false positives.
4.To evaluate the OpCyNet-DBRA framework against current machine learning and deep learning-based intrusion detection systems, showcasing its enhanced efficacy in cybersecurity applications.
5.To investigate the scalability and real-time application of the model, assuring its suitability for implementation in contemporary network contexts, including cloud and IoT-based infrastructures.
The remainder of the document is structured as follows: Section 2 addresses the connected works; Section 3 elaborates on the proposed approach; Section 4 examines the result analysis, and Section 5 presents the conclusion.

2. Related works

Dilshad et al. [18] present an innovative approach to improving DDoS attack detection by employing Federated Learning in model training and the Gini index for feature selection. The Gini index enhances model accuracy by removing extraneous features. Federated Learning enables scalable, decentralized training across multiple devices while preserving anonymity. The results endorse the application of this technology for detecting DDoS attacks, ensuring data confidentiality, and reducing computational load. The document indicates that the models achieved an average accuracy of 91%. Moreover, the implementation of our proposed strategy facilitated the detection of many types of DDoS attacks. The following precisions were achieved: 28.65% for DrDoS DNS, 28.94% for DrDoS SNMP, 9.20% for DrDoS UDP, and 20.61% for NetBIOS. This study predicts that IoV systems will meet current cybersecurity standards by integrating federated learning with improved feature selection. It provides a robust and efficient solution for the future automotive sector. To decentralize model training to devices and judiciously select only the most essential data features to minimize memory and time consumption. Consequently, the system is optimal for real-time IoV applications due to its enhanced speed and reduced resource use. Our method for recognizing DDoS attacks in IoV environments is both efficient and effective.

10.48047/jocaaa.2024.33.02.25

Current DDoS techniques, as noted by Pradeep & Shukla [19], are susceptible to False Positive Rates (FPR) and inadequately capture the complex patterns exhibited in attack traffic. The Internet of Things (IoT) is susceptible to several security threats, including DDoS attacks. Subsequently, the security frameworks and access control systems are enhanced by the integration of Software Defined Networking (SDN) with Internet of Things (IoT) models. DDoS attacks provide a substantial threat to IoT networks. This underscores the necessity to rectify the deficiencies of existing methods by creating a novel network anomaly detection model that employs a deep learning approach. The validation process commences with the extraction of essential validation metrics from the IDS ISCX 2012 dataset. The Predefined-Mud Ring Algorithm (P-MRA) is employed to select the optimal features from the input data. Optimally selected multi-serial characteristics. The CAE and GRU furnish the requisite attributes for validation. Subsequently, to assist the BL process in identifying network irregularities, these attributes are aggregated. The established framework has received numerous experimental validations, enhancing the traditional approach to anomaly detection in networks.

Kumar et al. [20] evaluated various models, including sequential and time-series elements, to identify DDoS attacks, compare different methods, and ascertain which is most likely to yield accurate predictions. They selected Long Short-Term Memory (LSTM) networks due to their demonstrated effectiveness in this domain. Utilize the CICDDoS2019 benchmark dataset, comprising 88 features, and extract a limited set of pertinent features (22 in total) prior to implementing supplementary deep learning models. The acquired outcome surpasses current methodologies attainable in this context through the application of data mining techniques, machine learning models, and certain strategies derived from the Internet of Things. While there is no infallible method to safeguard your server against these assaults, employing the approaches discussed thus far can mitigate their impact and enable your server to prioritize legitimate requests over those from fraudulent users.

Alfatemi et al. [21] propose a novel approach that integrates deep learning with Combinatorial Fusion Analysis (CFA) to enhance the identification of DDoS attacks. Four deep neural network models are developed for the binary classification of network traffic as either legitimate or a DDoS attack. The models analyze network traffic data by utilizing diverse input features to comprehend complex patterns. The probabilistic outputs of the four models are

10.48047/jocaaa.2024.33.02.25

integrated using CFA to enhance performance. This combinatorial technique enhances the accuracy of attack detection by efficiently aggregating the models' predictions. The proposed combinatorial integration of many deep learning models surpasses individual models and alternative ensemble methods in accuracy, based on comprehensive experiments performed on real-world network data. These findings illustrate the efficacy of combinatorial fusion in improving the detection of DDoS attacks through the integration of different deep learning models. This approach effectively mitigates the aggregate threat of distributed denial of service attacks.

Najar and Manohar Naik [22] proposed a novel hybrid architecture called "AE-CIAM" for the efficient detection and categorization of low-rate DDoS configurations. To diminish the complexity of the feature space and eliminate the need for human intervention, our system utilizes an Autoencoder (AE) enhanced with an attention module that adeptly extracts salient features from the data. Simplified attention autoencoders, unlike deep autoencoders, offer computational efficiency while maintaining complexity, rendering them appropriate for many purposes. Subsequently, to attain superior performance with less computing expense by employing the Attention Mechanism model to categorize attacks into several low-rate DDoS attack kinds. The CICIDS2017 dataset indicates an accuracy of 99.44% for multiclassification and over 99.99% for binary classification, showcasing exceptional efficacy. Furthermore, to assess our AE-CIAM model in relation to existing literature and showcase its superiority through several performance metrics.

3. Proposed Methodology

Figure 1 presents the workflow of proposed methodology for network traffic detection and each section is described in the following sub-section.

10.48047/jocaaa.2024.33.02.25

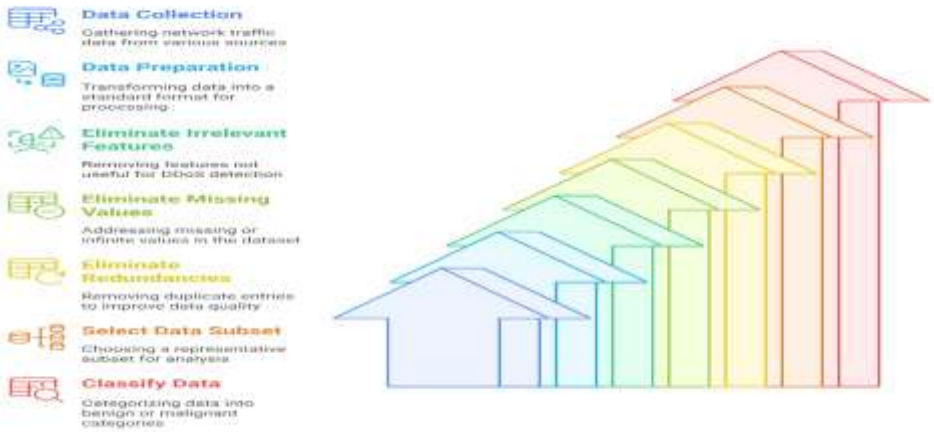

Figure 1: Workflow of Research Work

3.1 Data collection and Data Preparation

This study considers a freshly published extensive dataset that contains the latest information regarding DDoS assaults. The CICDDoS2019 dataset, just published, has been chosen as a resource [23]. This dataset comprises both benign and the latest authentic DDoS traffic characteristics to accurately replicate real-world data. The initial stage involves consolidating all recorded files into a singular dataset. The data must be in a standard format, such as a CSV file, to be imported and processed for model input. The existence of various data types, including numerical and categorical data, must be recognized. Data transformation is essential to provide uniform formatting, especially when handling extensive datasets, as issues such as incomplete or noisy data, substandard quality, and inconsistencies are unavoidable when aggregating network traffic data from many sources. The final stage of data preprocessing necessitates importing and evaluating the dataset, which involves data gathering executed by a Python application.

3.2 Data Preparation

This is a presentation of the data preparation techniques conducted on the dataset. To guarantee dependable results during model training, the subsequent step is to normalize and generalize the dataset.

10.48047/jocaaa.2024.33.02.25

3.2.1 Eliminate Irrelevant or Socket Features Unnamed: Zero, analogous HTTP include bits of socket information that are not particularly beneficial for identifying DDoS assaults; therefore, their elimination is the initial step. Training the model on the characteristics of packets is essential due to their variability across different networks. Consequently, of the 87 features, 79 remain pertinent for the model's input following the elimination of these eight features. Moreover, the identical IP address may be associated with both the offender and the ordinary user. The socket feature values employed to train the deep learning model may result in overfitting.

3.2.2 Eliminate/Replace Absent and Infinite Values

The original CIC-DDoS2019 dataset contains either an infinite or a substantial number of missing values due to its extensive volume. All of these values must be eliminated from the dataset. These feature values indicate attributes that influence the results of the training phase.

3.2.3 Eliminate Redundancies

Eliminating duplicates enhances data quality, redundancy, and integrity, hence facilitating more precise and reliable analysis through the preservation of the dataset. Significant duplicates exist in the original dataset, especially with the more recent DDoS attack type SSDP.

3.2.4 Arbitrary Selection Subset of Information

The limitations in computer applications, especially with analytical data and visualization difficulties, stem from the CIC-DDoS2019 dataset. Researchers often randomly select from subsets of datasets during studies. To randomly choose subsets for each attack type containing fewer than 150,000 instances subsequent to dataset cleansing. This subset of CIC-DDoS2019 was selected because to its comprehensive data sample and diverse range of attack types. Our findings are more comparable to the pertinent research due to the dataset being generated by writers from a reputable institution and the fact that numerous related studies conducted experimentation [24]. Nonetheless, among all the samples in the dataset, only 363 are classified within the range of 0.0003 for the WebDDoS attack type. To exclude it from the experiment due to its minimal dataset makeup and infrequent occurrence. It is less than other varieties. Furthermore, the disparate socioeconomic classes lack equilibrium. TFTP instances outnumber

10.48047/jocaaa.2024.33.02.25

all other types of attacks, despite LDAP instances being somewhat fewer in number. Subsequent to the cleaning step, a dataset including 1,060,572 records and 79 attributes was obtained. This dataset has twelve distinct groups. According to the principles of binary classification, the dataset is classified as either benign or malignant.

Table 1: Data split on a binary classification classical.

Training	**Class**	**Validation**	**Testing**
68584	Benign	7620	19051
695027	Malicious	77226	193064

3.2.5 Data Split

To enhance the assessment of the model's performance, the dataset, which consists of the gathered network traffic, is partitioned into three segments: a training set including 80% of the total and a testing set comprising 20%. Validation sets constitute 10% of the training process. After multiple tests, the ideal data splitting ratio was determined to be 80:20. Tables 1 and 2 present the segmented data for several classification models, encompassing both multiclass and binary categories. No consensus exists in data science over the optimal data-splitting ratio, as it is contingent upon size and lacks theoretical or numerical agreement. Our research extensively utilized data; nevertheless, just 20% of the dataset should be designated for testing to validate accurate predictions, while the remaining 80% should be allotted for training and validation purposes.

Table 2: Data split on a multiclass classification classical.

Class	Validation	Training	Testing
Multiclass-12	84846	763611	212115

3.3. Feature Scaling

10.48047/jocaaa.2024.33.02.25

The performance of classification models may be adversely affected by diverse uneven attribute scales. The feature scaling technique is employed during the input training data phase. It is a technique that reduces training data duration and addresses overfitting. Implement data normalization subsequent to the division of the dataset into training and test sets [25]. The dataset encompasses a broad spectrum of values, from exceedingly high to exceedingly low. The Min-Max Scaler transforms by normalizing each range to a scale of 0 to 1. This mitigates biases and prevents gradient vanishing and explosion. Subsequent to feature generalization, the model enhances both accuracy and precision. The Min-Max scaler can be represented by the formula in Equation (1).

$$X' = X - X_{min}/X_{max} - X_{min} \quad (1)$$

where X_{max} and X_{min} are the extreme besides minimum $feature\ values$ (X), output within the 0–1 range.

3.4. Classification: Optimized Cybernet Model Building (OpCyNet)

Concerning the proposed models, we will delineate our technique in this part. The major objective is to develop an innovative deep learning framework named Cybernet classical to evaluate the effectiveness and reliability of cybersecurity against cyber-DDoS attacks. This publication presented the OpCyNet DL model, utilized in this study. The proposed method comprises eleven trainable layers, including three fully connected layers and eight convolutional layers. One input layer constitutes the 33 layers that comprise this design. The proposed OpCyNet model's input layer accommodates 224x224 pixel images of agricultural pests. The initial convolutional layer applies a stride of 2x2 to the 224x224 input image for feature extraction. To optimize the convolutional kernels, partition the image into smaller regions. Kernels do a data traversal of the pest photos to generate the feature maps as output.

An expression for how the convolutional layer functions is

$$f_c^k(m,n) = \sum_d \sum_{r,s} j_d(r,s).\, i_c^k(v,w) \quad (2)$$

10.48047/jocaaa.2024.33.02.25

f_c^k represents the output feature map, $j_d(r,s)$ signifies the layer. The size is the result of applying convolutions on the input picture of the pest. Where i stands for input, p for padding, k for the size of the kernel, and s for the number of iterations.

Typically, activation functions come before convolutional layers. A layer node's activation function specifies how its input weight sum is transformed into an output. Rectified Linear Unit (relu) activation function layer. Since Relu activation is both effective and easy to implement, it is often employed. Here's how Relu functions:

$$f(x) = \begin{cases} 0, & x < 0 \\ x, & x \leq 0 \end{cases} (3)$$

After the initial convolutional layer, the LR activation functions are based on the subsequent convolutional layers. To avoid defining the function as (RAF) as a fraction of x. Following is the formula for determining this activation function.

$$f(x) = 0.01 \times x, x \ (4)$$

If the input is positive, the function returns x, but if returns 0.01 eras x. All convolutional layers are then followed by maximum pooling layers, which serve to reduce the computational complexity. Down-sampling is carried out by pooling layers to reduce the overall dimensionality. In order to increase the efficiency of the design and minimize over-fitting, this layer reduces the controls.

$$f(x) = max(x_1, x_2, x_3, .., x_k) \ (5)$$

Max-pooling is a down-sampling approach that uses a stride (s) to excerpt the maximum value image of size h w, where f(x) is an optimized feature vector. To reduce the number of training parameters and the final controls required by the network, a max-pooling layer is layered in among the convolutional layers to gradually reduce the size of the spatial representation, i.e., h and w. It's also useful for warding off over-fitting problems.

After using RAF, cross channel normalization, and output of the first layer is fed into the second. In the convolutional layer that follows, each of the 64 filters is 1 1. The inputs are filtered by 192 pixel in layer. The inputs to the fourth convolutional layer are passed through 512 kernels of size 3 3, with a 1 pixel padding value and a 2-pixel stride. The inputs to the fifth

10.48047/jocaaa.2024.33.02.25

convolutional layer are passed through 384 kernels of size 3 3, padded and stride by 1 pixel. There are no pooling layers beyond the sixth, seventh, or eighth convolutional layer, which each apply 256 pixel. FC layers receive feature maps extracted by these layers. Each FC layer's nodes are connected to those of the next higher layer. The retrieved 2-D feature map is feature vector using FC layers. The operation of the FC layer is shown in Equation 6.

$$a_i = \sum_{j=0}^{m \times n^{-1}} w_{ij} \times x_i + b_i \quad (6)$$

where n, m, d, and i represent the height, breadth, depth, besides directory of output, respectively. Moreover, the bias and weights are indicated by b and w, respectively. Following the layers are the LR and dropout layers, followed by the softmax and classification layers. Since our data is divided into twelve classes, the final FC layer's output is sent on to a 12-way softmax.

3.5. Fine-tuning using Developed Battle Royale Optimization Algorithm (DBRA)

This work uses DBRA to fine-tune CyNet model parameters, starting with BRA. Battle Royale, inspired by a Japanese film, is a popular and demanding multiplayer online battle arena game. This game requires you to see everything to survive. Battle Royale can be played solo, with a companion, or in a five-person squad. Because of the game, all players start with the same skills and goods. Participants' locations are also randomly selected at the start of the game. The playable area shrinks with time, and players who wander outside risk being eliminated or injured. One organization or person can win. In Player Unknown's Battlegrounds, Sanhok is a common map choice. By staying close in the game's blue-outlined "safe zone," often known as "the circle," players avoid being harmed and receiving damage ticks. White circles represent smaller buffer zones as they decline. Players actively seek out and eliminate opponents to continue. One of Player Unknown's Battlegrounds' game types asks players to kill a particular number of opponents in a certain time. In this "death match" phase, the winner removes the most opponents. Additionally, the eliminated player may appear unexpectedly on the field. Some games start when the participant parachutes or planes into the field.

Optimizing for the Battle Royale: The population used in the algorithm begins with a uniform distribution over the study area. Based on his position, each soldier fires at and injures the other troops in his immediate vicinity, increasing their damage by one (damage = z_j.damage + 1).

10.48047/jocaaa.2024.33.02.25

The wounded soldier wants to quickly relocate so he may begin firing on the enemy from a different flank. So that he may concentrate on exploitation, the soldier is stationed midway between the previous site and the finest location discovered. Here to provide the mathematical equation for these behaviors [26]:

$z_{dam.d} = z_{dam.d} + r(z_{best.d} - z_{dam.d})$ (7)

z_(dam.d) has dimension d and represents the site of the wounded soldier; r is a random sum in the intermission [0, 1]. If the wounded soldier is able to kill the enemy in the next cycle, z_j will be equal to 0. If the jth soldier's damage total (z_j) in the exploration phase is more than a certain threshold value, z_j dies but may reappear at random in area, and z_j. damage may decrease to 0. The threshold quantity of three was arrived at by error. This promotes healthy examination and stops people from merging too soon. To represent a dead soldier's appearance in the search space, to use the following expression.

$z_{dam.d} = r \times (ub_d - lb_d) + lb_d$ (8)

The bounds in problem space are designated by ub_{d} and lb_{d}. The early sum of problematic space is $w = log_{10}(MaxCicle)$ with problem develops smaller rendering to the finest solution and its value is $w = w + round\ (\frac{w}{2})$. Supreme amount of generation is articulated by MaxCicle.

The efficient bound below:

$lb_d = z_{best.d} - SD(\overline{z_d})$ (9)

$ub_d = z_{best.d} - SD(\overline{z_d})$ (10)

Where z_(best.d) is the best key ever discovered in dimension d and SD((z_d)) is the population standard deviation, the computing cost of the proposed technique is proportional to the dimensions of the issue, the largest sum of epochs, and the populace size. The greatest soldier from each era is preserved as a member of a select group.

3.5.1. Developed Battle Royal Optimization Procedure

10.48047/jocaaa.2024.33.02.25

The innovative Battle Royal Optimization Procedure produces powerful analysis but may perform poorly in other contexts, such as incorrect local optimal outcomes [26]. The SOFC mathematical model [26] requires an efficient model estimator, therefore this work performed two sorts of improvements to improve the process. OBL underpins the first enhancement. Treat each pair of developed solution candidates as the primary candidate's complement using OBL.

$$\vec{z}_j^{new} = \vec{z}_j^{max} + \vec{z}_j^{min} - \vec{z}_j \quad (11)$$

where $\vec{z}_j^{new}$ labels the opposite position of $\vec{z}_j$, and $\vec{z}_j^{min}$ define the least an $\vec{z}_j^{max}$ is the higher limits of the key.

In each pair, we'll choose the best option and ditch the other one until to have a single viable contender.

Here, the OBL mechanism accounts for 40% total population while random selection accounts for 60% of the original population. "Chaos theory" is the other enhancement employed here. This approach does not produce really random numbers, but rather pseudo-random ones. The metaheuristics may utilize this to improve the algorithm's convergence rate. The literature introduces several forms of chaos. A sinusoidal map was created for this analysis. The formula for the update of Equation (12) may be written as follows, with the r parameter serving as a pseudo-random variable.

$$r_1(j+1) = P \times r_1^2(j) \times sin(\pi \times r_1(j)) \quad (12)$$

where the chaotic random charge shaped in the contemporary repetition is defined by r_1 (j+1), and the chaotic chance value produced in previous iteration is defined by r_1 (j). Here, we've set P = 2.2 r_1 (0) to 0.6.

4. Results and Discussion

The DDoS attack detection approach uses common performance measurements. These models were created using a PC with a 12th-generation Intel Core i7-12650H 2.30 GHz processor, 16 GB RAM, 2X512GB SSD, and Windows 10. Tensorflow-gpu must be installed on Python to use models [27]. After that, report your observations and discuss the suggested models.

10.48047/jocaaa.2024.33.02.25

Subdividing the dataset into subsets followed normalization and model application. To test the models with industry-standard performance measures and find them effective.

4.1. Analysis of Proposed model on Binary Class

Figure 2 mentions the graphical analysis of projected model on binary attack detection in terms of diverse metrics.

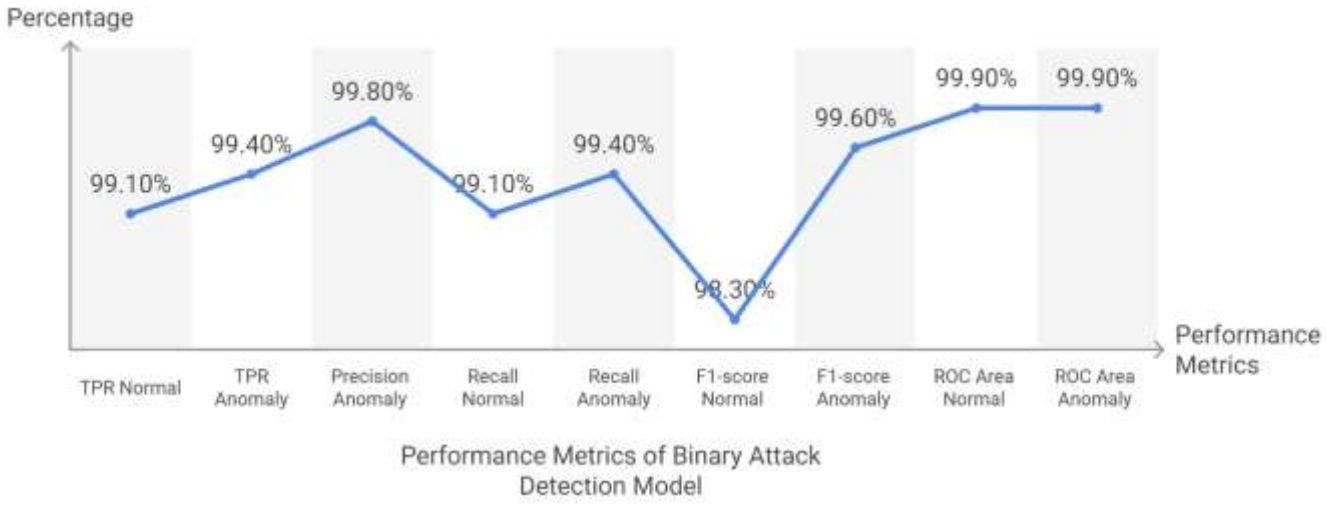

Figure 2: Visual Analysis of planned model on binary class

True Positive Rates (TPR) of 99.10% and 99.40% for normal and abnormality classes indicate great detection accuracy in binary classification. Precision for anomalies is 99.80%, ensuring few false positives, and Recall values (99.10% for normal and 99.40% for anomaly) indicate great sensitivity to both categories. F1-scores of 98.30% (Normal) and 99.60% (Anomaly) suggest balanced precision and recall, ensuring trustworthy categorization. Both classes have 99.90% ROC Areas, indicating near-perfect discrimination. The model performs well in binary classification with few false positives and great robustness in discriminating normal and anomalous occurrences.

4.2. Validation Analysis of proposed classical on multi-class

10.48047/jocaaa.2024.33.02.25

The investigation of proposed classical on multi-class attack is verified in terms of different metrics and it is exposed in Figure 3.

Figure 3: Graphical Comparison of various attack class in proposed classical

The multi-class classification results show strong performance in most classes, with True Positive Rates (TPR) from 46.20% to 100.00% and Precision values up to 100.00%. Consistently high ROC Area (≥99.10%) indicates strong discrimination ability. Class 2 and Class 9 have lesser recall (46.20% and 50.00%, respectively), suggesting identification issues. The model classifies instances accurately with high confidence due to the high precision values. The model performs well for multi-class recognition with low false positives (FP Rate = 0.00% for most classes), high recall, and strong F1-scores.

5. Conclusion

Employing the CICDDoS2019 dataset, this study introduces a novel methodology for network attack detection termed the Optimized Cybernet Model (OpCyNet), which integrates the

10.48047/jocaaa.2024.33.02.25

Developed Battle Royale Optimization Algorithm (DBRA). The primary purpose was to employ a cutting-edge deep learning framework to enhance cybersecurity's capacity to detect and mitigate DDoS attacks. The OpCyNet model comprises three fully connected layers and eight convolutional layers, resulting in a total of eleven learnable layers in this deep learning architecture. The model employs multiple layers, such as max-pooling, dropout, batch normalization, leaky ReLU, and softmax, to effectively extract high-level feature representations. The model is trained on network traffic utilizing rectified activation functions (ReLU and LR) alongside cross-channel normalization. The DBRA was employed to boost both model accuracy and computational efficiency through improved feature selection and classification optimization. DBRA's elimination of extraneous parameters and focus on the most distinguishing features enhances OpCyNet's generalization, reduces overfitting, and increases attack detection accuracy. In comparison to conventional deep learning and machine learning methodologies, the OpCyNet-DBRA model demonstrates much superior performance on the CICDDoS2019 dataset regarding attack detection score and false positive rate. To protect real-world cybersecurity applications from evolving DDoS attacks, our hybrid method provides a sophisticated, efficient, and scalable solution. This work demonstrates that integrating deep learning-based threat detection with metaheuristic optimization significantly enhances cybersecurity resilience. Future research can enhance IDS performance in dynamic cyber environments by investigating adversarial robustness, cross-dataset validation, and real-time deployment.

References

[1]H.T.Manjula,Neha Mangla An Approach to on stream DD0S blitz detection using machine learningalgorithmsMaterialsElsevierToday:Proceedingshttps://doi.org/10.1016/j.matpr.2021.07.280

[2] H.T.Manjula,Neha Mangla An Effectual Cram DDos Blitz Tools and Approach via Hadoop Framework,Volume 15 Issue 8 2020 Syebold report ISSN No:1533-9211

[3] Liu, L. (2024). identification and evaluation of processing system cybersecurity issues. Environmental Protection and Process Safety, 185, 1061-1071.

[4] Tiwari, V. K. (2023, October). Using a Hybrid Feature Selection Based Modified Convolutional Neural Network to Identify Anomaly Attacks in Industrial IoT. Evolutionary

10.48047/jocaaa.2024.33.02.25

Algorithms and Soft Computing Techniques International Conference (EASCT) 2023 (pp. 1–7). IEEE.

[5] Uddin, M. A. (2024). IDS framework with an effective unknown attack detection focus based on usfAD. 14(1), Scientific Reports, 29103.

[6] Abdulhameed, A. A. (2024). A Comprehensive Review of the Literature on Software-Define Networking (SDN) Cyberattack Detection. Journal of Cybersecurity in Mesopotamia, 4(3), 86–135.

[7] Gregus, M. (2024). assessing deep learning variations for multi-class classification and cyberattack detection in IoT networks. 10, e1793, PeerJ Computer Science.
[8] Vaneeta, M. (2021). Bayesian hybrid detection in MANET for effective malicious node intrusion detection. Materials Science and Engineering, IOP Conference Series (Vol. 1022, No. 1, p. 012077). IOP publishing.

[9] Zhao, J. (2024). Textual Analysis of Volt/VAR Commands for Smart Inverter Cyber-Attack Detection Using a Large Language Model. IEEE Smart Grid Transactions.
[10] Yamarthy, A. K. (2024). To improve cyber security, MDepthNet-based phishing attack detection employs integrated deep learning techniques. Cluster Computing, 1–19.
[11] Albuquerque, V. H. C., & Gupta, D. (2022, October). Intrusion detection in cyber-security networks is based on deep learning techniques. MysuruCon, IEEE 2nd Mysore Sub Section International Conference, 2022 (pp. 1–7). IEEE.

[12] Sampathkumar, B. (2024, April). Deep learning and anomaly detection methods are used to identify cybersecurity threats. Volume 1, pages 1–7, 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS). IEEE.
[13] Khalghani, M. R. (2024). Power distribution grid cyberattack detection using an unsupervised adversarial autoencoder. Research on Electric Power Systems, 232, 110407.
[14] R. Doriguzzi-Corin (2024). FLAD: adaptive federated learning for the detection of DDoS attacks. Security & Computers, 137, 103597.

[15] Nhung-Nguyen, H., & Najar, A. A. (2024). Deep neural networks in an SDN context are used for DDoS attack detection and mitigation. Security & Computers, 138, 103661.
[16] Naqvi, S. A. R. (2024, December). Enhancing Cyber-Attack Identification in Power

10.48047/jocaaa.2024.33.02.25

Systems: A Comparison of Graph Neural Network and Machine Learning Methods. Resilience Week (RWS), 2024 (pp. 1–9). IEEE.

[17] Behal, S., and B. Bala (2024). AI methods for detecting DDoS attacks on the Internet of Things: classifications, thorough analysis, and research issues. 52, 100631, Computer Science Review.

[18] Dilshad, M. (2025). Effective Detection of Distributed Denial of Service Attacks in Internet of Vehicles Through Federated Learning and Gini Index Feature Selection. Internet of the Future, 17(1), 9.

[19] Pradeep, K. J. (2025). utilizing multi-serial stacked networks and the best feature selection techniques to fend off DDOS attacks to create a revolutionary network anomaly detection framework. Intelligent Networks International Journal, 6, 1–13.

[20] Kushwaha, C., and Sethi, D. (2025). examining how well multivariate LSTM models perform in forecasting the likelihood of Distributed Denial of Service (DDoS) attacks. e0313930 in PloS One, 20(1).

[21] Solyman, A., Alfatemi, A., Rahouti, M., Hsu, D. F., Schweikert, C., Ghani, N., & Assaqty, M. I. S. (2025). Combinatorial analysis and multi-model deep learning fusion are used to detect distributed denial of service attacks. Network and Systems Management Journal, 33(1), 8.

[22] Manohar Naik, S., and Najar, A. A. (2025). A hybrid AI-enabled framework for cloud computing low-rate DDoS attack detection is called AE-CIAM. 103 in Cluster Computing, 28(2).

[23] Khan, M. N. A., Saluja, K., Bagchi, S., Solanki, V., Dhamija, E., & Debnath, S. K. (2024, August). Using the CICDDoS2019 Dataset, a machine learning analysis is conducted to investigate robust DDoS detection. India Council International Subsections Conference (INDISCON), IEEE 5th, 2024 (pp. 1-6). IEEE.

[24] Aluvalu, R., Thirumalraj, A., Uma Maheswari, V., Stephe, S., & Mohanty, S. N. (2024). Advanced AI methods for COVID-19 illness identification from CT scan pictures are based on the Chaotic Satin Bowerbird optimizer. 1065–1087 in New Generation Computing, 42(5).

[25] Kavin Balasubramanian, P. (2024). A case study on IoT-enabled waste management in smart cities using an optimized deep learning framework facilitated by NMRA. In Advancements for Intelligent Systems of the Future for Sustainable Development (pp. 247-268). IGI Worldwide.

10.48047/jocaaa.2024.33.02.25

[26] Karamnejadi Azar, K., & Ghadamyari, M. (2022). designed a battle royale optimizer to find solid oxide fuel cells as efficiently as possible. 9882 in Sustainability, 14(16). [27] Nagarathinam, K. (2024). Original Research Article: Using ADSY-AEAMBi-LSTM with DBO feature selection to detect data imbalance in MANET networks. Autonomous Intelligence Journal, 7(4), 1094.

Authors' Contributions

Mrs Manjula HT Conceptualization, methodology, investigation, writing—original draft preparation. Dr Jyoti Metan Conceptualization, methodology. writing—original draft preparation,