ANOMALY DETECTION IN NEXT-GEN IOT:GIANT TREVALLY OPTIMIZED LIGHTWEIGHT FORTIFIED ATTENTIONAL CONVOLUTIONAL NETWORK

Dr. K. SUJATHA[1*], Dr.KALYANKUMAR DASARI[2], S. N. V. J. DEVI KOSURU[3], NAGIREDDI SURYA KALA[4], Dr. MAITHILI K[5], Dr.N.KRISHNAVENI[6]

[1*]Assistant Professor,Department of CSE,CSE, SRMIST Ramapuram
[2]Associate Professor & HOD,Department of CSE-CS,C halapathi Institute of Technology ,Mothadaka, Guntur,India
[3]Assistant Professor,Department of CSE,Koneru Lakshmaiah Education Foundation Vaddeswaram-522302, Guntur, Andhra Pradesh, India
[4]Assistant Professor,Department of Information Technology,Aditya College of Engineering & Technology (A)Surampalem-India
[5]Associate Professor,Department of CSE(AI & ML)KG Reddy College of Engineering and TechnologyHyderabad, Telangana, INDIA-500086
[6]Assistant Professor,Computer Science and Engineering,Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology,Chennai ,India
[1*]Corresponding author email: sujathak14.97@gmail.com

ABSTRACT

Within the most recent version of security monitoring solutions crafted for interconnected device networks faces limitations due to data scarcity, diverse device types, and limited computational resources. Unlike traditional solutions, these networks require a different approach. To address these limitations, the paper introduces LF-ACANet-GTOA, a novel approach leveraging a unique architecture called Lightweight Fortified Attentional Convolutional Network. This model is optimized with the Giant Trevally Optimization Algorithm (GTOA) for efficient and accurate intrusion detection within resource constrained IoT networks. The system focuses on critical information within network traffic data using an attention mechanism. It analyses two public datasets such as CIC-IDS-2017 and Bot-IoT to assess the effectiveness of LF-ACANet-GTOA. A meticulous pre-processing stage ensures clean and consistent data for the model. It provides a detailed description of the LF-ACANet-GTOA design, encompassing its components: Convolutional Encoder, Feature Enrichment Block, Attention Mechanism Integration, and Classification Layer. Additionally, it utilizes the Giant Trevally Optimization Algorithm (GTOA) for efficient training and optimization. The simulation results for the proposed LF-ACANet-GTOA method on the CIC-IDS-2017 dataset are promising, achieving high accuracy (99.57%), precision (99.26%), recall (99.16%), and F-score (99.21%), with low false alarm (0.73%) and miss rates (0.83%). These results suggest that LF-ACANet-GTOA has the potential to be a robust and secure solution for intrusion detection in resource-constrained interconnected device networks.

Keywords: *Security monitoring solutions, Interconnected device networks, Lightweight Fortified Attentional Convolutional Network (LF-ACANet-GTOA), Giant Trevally Optimization Algorithm (GTOA), CIC-IDS-2017 and Bot-IoT.*

1. INTRODUCTION

LF-ACANet-GTOA tackles the challenge of intrusion detection in IoT networks by leveraging a unique architecture specifically designed for this purpose. This architecture prioritizes lightweight design principles to ensure efficient operation on devices with limited processing power, ensuring smooth integration within the IoT ecosystem.

Furthermore, it incorporates an attention mechanism that focuses on crucial information within network traffic data, enhancing the efficacy of the proposed LF-ACANet-GTOA model in discerning benign from malicious behaviors.

Finally, the model is optimized using Giant Trevally Optimization (GTOA), an influential algorithm modeled after the predatory strategies observed in giant trevally fish. GTOA facilitates efficient training by guiding the optimization process towards configurations that minimize loss and maximize intrusion detection accuracy.

This innovative combination offers a lightweight, accurate, and efficient approach to intrusion detection, significantly bolstering security in the ever-evolving realm of IoT.

The remaining sections of this manuscript explore the details of proposed LF-ACANet-GTOA method: Section 2 delves into prior studies on interconnected devices intrusion detection. Section 3 elaborates on proposed LF-ACANet-GTOA methodology, including its architecture, attention mechanism, and optimization algorithm. Section 4 evaluates LF-ACANet-GTOA performance through experiments and presents the results and Section 5 wraps up research by summarizing findings, acknowledging limitations, and proposing pathways for future exploration.

2. RELATED WORKS

Numerous recent studies have investigated for detecting Intrusion detection in IoT. Below are some of the recent studies closely related to this topic,

In 2023, Thakkar, A. and Lohiya, R., [21], suggested the Imbalanced Security monitoring solutions in Interconnected device networks utilizing ensemble learning with deep neural networks (ELBC-DNN). The article aimed to tackle the challenge of class imbalance using an ensemble learning method called the bagging ensemble harnesses the power of a deep neural network for robust classification. Their approach modified the DNN training process by integrating class weights to ensure balanced training subsets. This approach offered a dual benefit by striving for generalization while addressing class imbalance in intrusion detection datasets. However, it achieved a low error rate with a low F-Score value.

In 2023, Nguyen, D.T. and Le, K.H., [22] suggested the Decision Tree based resilient approach to detecting intrusions in Internet of Things networks (DT). In this, the objective was to evaluate the effectiveness of the resilient decision tree in challenging IoT environments. Initial tests indicated sensitivity to the offset parameter, prompting the implementation of a statistical method for automatic offset value selection to enhance model stability across different attack offsets. Subsequently, a robust IDS framework for IoT settings was introduced, combining the enhanced resilient decision tree with a tabular deep learning model for detecting and classifying various cyber-attacks. However, it attained a low false alarm rate with a low F-Score value.

In 2023, Nguyen, X.H. and Le, K.H., [23] presented Detecting Unknown Denial-of-Service Attacks in Interconnected device networks with a SOCNN-LOF-iNNE Learning Model (SOCNN-LOF-iNNE). In this scenario, the system combines a supervised SOCNN for feature extraction with unsupervised LOF and iNNE for anomaly detection, capitalizing on both learning paradigms. Furthermore, it showcased resilience against adversarial attacks, indicating its potential to bolster Interconnected device networks security designed to safeguard against DoS/DDoS attacks in evolving threat environments. However, it achieved a low accuracy value with a high F-Score value.

In 2023, Bakhsh, S.A. et.al., [24] presented Augmenting security in Interconnected device networks via deep learning-driven Intrusion Detection System. Here, it investigated the application of artificial neural networks, including Feedforward, Long Short-Term Memory, and Random architectures, for enhancing the cybersecurity of interconnected device networks. Each DL model offers distinct advantages: FFNN handles intricate IoT network traffic patterns, LSTM captures extended dependencies in network traffic, and RandNN adapts and learns from data through harnessing randomness and dynamism. These algorithms revolutionize cybersecurity by providing adaptable shields against escalating cyber threats, ensuring data integrity in the burgeoning IoT space. However, it achieved a high accuracy value with a high computation complexity.

In 2024, Li, S. et.al [25] suggested HDA-IDS: A Hybrid Approach for IoT DoS Attack Detection Leveraging Semi-Supervised CL-GAN Technique. By merging Known threat detection and behavioural anomaly identification, this approach broadens its scope to encompass both established and zero-day DoS/botnet attacks. Furthermore, it familiarized a Behavioural deviation detection system named CL-GAN, a generative model combining CNN-LSTM with GAN architecture, establishes a baseline for normal traffic patterns and detects anomalies suggestive of malicious activity. However, it achieved a high miss rate.

In 2023, Vishwakarma, M. and Kesswani, N., et.al [26] suggested dual-stage Security monitoring solutions leverages Naive Bayes for categorization alongside the elliptic envelope technique for anomaly identification. Initially, data was categorized into four types (nominal, integer, binary, float) and classified using various Naive Bayes classifiers. Leveraging a majority vote for final class labels, the system then analyses benign traffic from stage one using an unsupervised elliptic envelope for anomaly detection. However, it achieved a low accuracy value with a high Recall value.

In 2022, Saheed, Y.K. et.al [27] utilized machine learning within a Security monitoring solutions to identify Digital assaults on the Interconnected device networks. The study sought to harness ML-supervised algorithms for IoT intrusion detection. Initially, the data underwent feature scaling via min-max normalization to avoid information leakage during testing. This dataset included various types of network traffic, incorporating contemporary attacks and normal activities, classified into nine attack categories. Following this, PCA was leveraged to extract the most significant features from the data. Finally, six machine learning models were applied for analysis. However, it achieved a low F-Score value with a high Precision value.

3. LF-ACANet-GTOA MODEL CONSTRUCTION PROCESS

Here, the construction process behind the Lightweight Fortified Attentional Convolutional Network with Giant Trevally Optimization for Adversary-Aware Intrusion Detection in IoT Networks (LF-ACANet-GTOA) is discussed. It is designed specifically for efficient and accurate intrusion detection within resource-constrained Internet of Things (IoT) networks. This model leverages two publicly available datasets for training and evaluation. The block diagram of the proposed LF-ACANet-GTOA methodology is given in Figure 1. The detail description about each stage is given below,

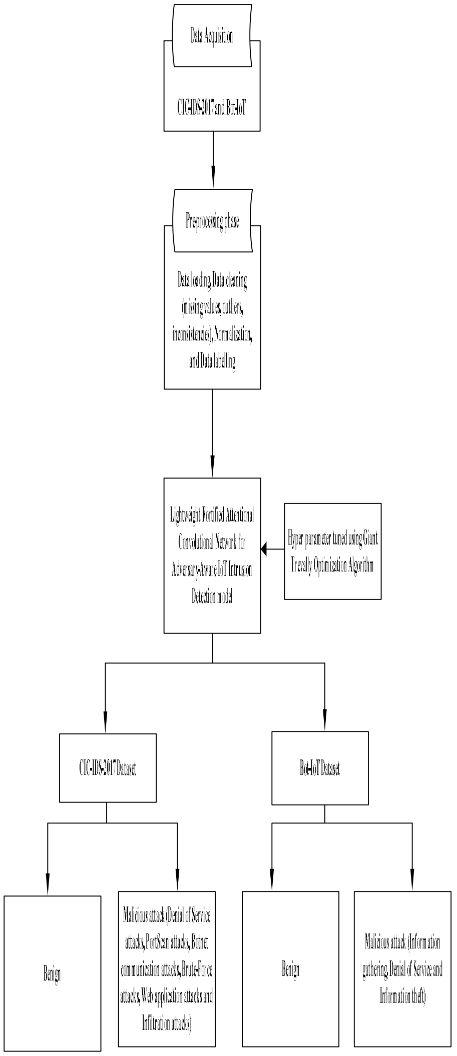
Data Acquisition
CIC-IDS-2017 and Bot-IoT
Pre-processing phase
Data loading, Data cleaning (missing values, outliers, inconsistencies), Normalization, and Data labelling
Lightweight Fortified Attentional Convolutional Network for Adversary-Aware IoT Intrusion Detection model
Hyper parameter tuned using Giant Trevally Optimization Algorithm
CIC-IDS-2017 Dataset
Bot-IoT Dataset
Benign
Malicious attack (Denial of Service attacks, PortScan attacks, Botnet communication attacks, Brute-Force attacks, Web application attacks and Infiltration attacks)
Benign
Malicious attack (Information gathering, Denial of Service and Information theft)

Figure 1: Diagram illustrating the proposed LF-ACANet-GTOA methodology.

3.1 Data acquisition

To assess the competence of Security monitoring solutions in the context of the Interconnected device networks, this study examines two notable datasets: CIC-IDS-2017 and Bot-IoT. The detail description about the dataset is given below,

3.1.1 CIC-IDS-2017 Dataset

The CIC-IDS-2017 dataset is provided by the Canadian Institute for Cybersecurity (CIC), which contain real-world IoT network activity. Logs from a controlled Interconnected device networks ecosystem populated with various IoT devices. It offers a emulated network behaviour mirroring real-world scenarios patterns encountered in deployed IoT networks. The dataset includes benign, and various Denial-of-Service (DoS) attacks aimed at disrupting network operations [28]. The dataset likely also contains Infiltration attack, Brute-Force attacks and Web application attacks exploiting vulnerabilities in IoT devices. Additionally, the dataset encompasses other IoT-specific attacks such as PortScan or botnet communication used by attackers to control compromised devices. The Overview of Statistics for the CIC-IDS-2017 data utilized for this analysis is presented in Table 1.

Table 1: Overview of Statistics for the CIC-IDS-2017 dataset

Name of the attack		**Total**
Benign		2,273,097
Denial of Service attacks	Distributed denial-of-service (DDoS) attacks alongside exploit techniques like Heartbleed and various DoS tools (slowloris, Slowhttptest, Hulk, GoldenEye)	3,80,699
PortScan attacks	PortScan	158,930
Botnet communication attacks	Bot	1966
Brute-Force attacks	FTP and SSH protocols	13,835
Web application attacks	SQL Injection, Cross-Site Scripting (XSS) and Brute Force	2,180
Infiltration attacks	Infiltration	36
Total		2,830,743

3.1.2 Bot-IoT

The Bot-IoT dataset Offered by Northeastern University, which offers a comprehensive look into real-world network behaviour, focusing specifically on security threats targeting Internet of Things (IoT) devices. It meticulously captures both normal network activity and various cyberattacks launched against diverse devices, including Ubuntu servers, mobile phones, and smart home appliances [29]. It encompasses information gathering techniques like port scanning and operating system fingerprinting, allowing attackers to identify vulnerabilities in targeted systems. Denial-of-service attempts are also simulated, showcasing methods like flooding networks with traffic to overwhelm and disable them. Additionally, the dataset includes information theft attacks, where attackers exploit vulnerabilities to steal sensitive data. The breakdown of attack categories within the Bot-IoT dataset reveals a focus on probing attacks, denial-of-service attacks, and information theft attacks. The Overview of Statistics for the Bot-IoT data utilized for this analysis is presented in Table 2.

Table 2: Overview of Statistics for the Bot-IoT Database

Name of the attack		**Total**
Benign		9543
Reconnaissance	Network reconnaissance	1463364
	Operating system Signature extraction	358275
Denial of Service	Multi-vector DDoS attacks exploiting transport (TCP, UDP) and application layer (HTTP) protocols	3,85,32,480
	DoS (TCP, UDP, HTTP)	3,30,05,194

Information misappropriation	Unauthorized keystroke capture	1469
	Data exfiltration	118
Total		7,33,70,443

3.2 The starting step of Data preparation

In this section, the starting step of Data preparation including data loading, cleaning (missing values, outliers, inconsistencies), normalization, and labelling is discussed, that prepare the dataset for the proposed LF-ACANet-GTOA intrusion detection model. This meticulous process ensures clean, consistent data suitable for the model's learning. It begins by leveraging pandas from python to load the dataset. This creates a structured DataFrame for easier manipulation. Next comes data cleaning. Missing values are identified and addressed by removal or imputation using techniques like mean/median/mode.

Data points that deviate significantly from the norm, often referred to as outliers, can potentially mislead the model. SciPy's Interquartile Range (IQR) method helps identify these outliers. IQR represents the variability within the central half of the statistics. Values outside a specific range, typically data points falling outside the range of 1.5 times the IQR from the middle 50%, are indicated [30]. With the help of this, outliner is removed. Inconsistencies in format or typos are rectified using pandas' string manipulation capabilities. After a thorough cleaning, normalization ensures all features contribute equally during the training of the LF-ACANet-GTOA model. Here, Scikit-learn's StandardScaler standardizes numerical features to a common range, typically centered around an average value of zero and exhibiting a standard variation of one, this normalization prevents features with larger scales from overshadowing the learning process, enabling the model to treat all features equally. It is represented in equation (1)

$$\text{New value} = \frac{(\text{Original value} - \text{Mean})}{\text{Standard deviation}} \qquad (1)$$

Where Original value is the value of a data point before normalization; Mean reflects the average value of all data points within the feature (column). $\text{Standard deviation}$ represents the standard deviation of all data points in the feature. Normalization through StandardScaler ensures that all numerical features are on a level playing field, facilitating faster convergence and more efficient learning for the LF-ACANet-GTOA model.

Finally, data labelling process is done. If the dataset lacks pre-existing labels, Security Analysts assign labels based on attack types. These labels can be "normal" for typical network traffic or specific attack names like "denial-of-service (DoS)". Their expertise in network traffic patterns and intrusion detection is crucial for accurate labelling. LabelEncoder from scikit-learn then transforms these categorical labels into numerical values suitable for the proposed LF-ACANet-GTOA model. The proposed LF-ACANet-GTOA model require numerical data for processing, and LabelEncoder performs a simple mapping for this purpose. For example, "normal" might be converted to 0, and "DoS attack" to 1.

By following these meticulous pre-processing steps, the data becomes clean, consistent, and ready to be fed into the proposed LF-ACANet-GTOA model. This well-prepared data lays the foundation for the model to learn effectively and ultimately achieve robust performance in intrusion detection.

3.3 LF-ACANet-GTOA Design for Adversary-Aware IoT Intrusion Detection

In this section, Lightweight Fortified Attentional Convolutional Network for Adversary-Aware IoT Intrusion Detection (LF-ACANet) model optimized with Giant Trevally Optimization Algorithm (GTOA) (LF-ACANet-GTOA) is discussed. This model tackles IoT network intrusion detection by leveraging its unique architecture. The LF-ACANet-GTOA model consists of an input layer, a convolutional encoder, Feature Enrichment Block, Attention Mechanism Integration, and Classification Layer. The detail description about each layer is given below,

Input layer:

The input layer receives pre-processed network traffic data samples from the IoT network. These samples are labelled as either benign or a specific attack type.

Convolutional encoder module:

Then the pre-processed data will be fed through the convolutional encoder module. This module consists of stacked convolutional layers to extract low-level features from pre-processed network traffic data like Packet sizes (bytes), Connection details including IP addresses, ports, and protocols (TCP, UDP, etc.), timestamps. Each convolutional layer performs a convolution operation, and it is mathematically represented in equation (2)

$$Data_{Ch}^{la} = \sigma_1\left(\sum_{Ch' \in F_{la}} Data_{Ch'}^{la-1} * K_{Ch',Ch} + Bias_{Ch}\right) \tag{2}$$

Where, $Data_{Ch}^{la}$ represents the activation at channel Ch in the current data representation (la); σ_1 represents the activation function; F_{la} specifies the number of channels extracted by layer $la, Data_{Ch'}^{la-1}$ represents the Input value at channel Ch of the previous feature map ($la-1$). $K_{Ch',Ch}$ represents the Value at position Ch of the filter kernel in layer la. Bias term $Bias_{Ch}$ for channel Ch in the current feature map. This equation (2) essentially calculates the weighted sum of previous feature map $Data_{Ch'}^{la-1}$ convolutional with filter kernel $K_{Ch',Ch}$ followed by adding the bias $Bias_{Ch}$, capturing local traffic patterns within the encoder. After the convolution, a non-linear activation step (like ReLU) is employed to introduce non-linearities. [31]. This function is mathematically represented in equation (3)

$$\sigma\left(Data_{i,Ch}^{la}\right) = \max\left(0,\ Data_{i,Ch}^{la}\right) \tag{3}$$

This equation (3) ensures non-linearity. Here, $\sigma\left(Data_{i,Ch}^{la}\right)$ shows the result for channel i after passing through the activation function in the present data representation. By setting negative values to zero, ReLU empowers the model to identify sophisticated dependencies within the features compared to linear activation. By this, convolutional encoder progressively extracts traffic features via convolution and activation, feeding them for attack classification.

Feature Enrichment Block (FEB)

This block plays a crucial role in capturing intricate features essential for identifying diverse attack patterns. It achieves this capability through a technique called atrous convolution. Generally, Standard convolution in CNNs reduces the detail of data feature (granularity) as layers progress. So, Atrous convolution were employed to counteracts this by capturing features across a larger span while preserving local details, enabling more comprehensive analysis of network traffic. This FEB architecture empowers the proposed LF-ACANet-GTOA model to extract a wider range of features across the entire traffic data representation. These features capture valuable spatial relationships within the data, providing a richer context for differentiating between benign and malicious traffic patterns. The mathematical representation for atrous convolution is given in equation (4),

$$y[i] = \sum_{K=1}^{N}\left(Data\left[i + RP * K\right] * w[K]\right) \tag{4}$$

Where $y[i]$ depicts the Outcome at channel i in the transformed data captures the model's interpretation; $Data[i]$ corresponds to the initial value for element i in the unprocessed data representation; $w[K]$ corresponds to the coefficient at position K of the convolution kernel; RP depicts the Dilation rate parameter which controls the spacing between filter elements; K represents the Index iterating over the filter kernel elements. This equation (4) utilizes a dilated filter to capture features across a wider range of the data. This approach preserves the original granularity within the data. By incorporating the FEB with atrous convolution, the proposed LF-ACANet-GTOA model enhances its ability to detect various attack patterns within the network traffic data by extracting informative features at different scales and preserving crucial spatial information.

Attention Mechanism Integration:

The output of the FEB will be used in the Attention Mechanism Integration (attention-guided decoder module). This decoder focuses on the most critical information for identifying intrusion patterns within the IoT network traffic data. It employs Up-Block layers to progressively increase the size of the feature maps. This expansion allows for more precise localization of attack patterns within the traffic data. Also, it integrates a attention mechanism. This mechanism leverages an additional input denoted by Z from the network's lower layers. This Z input serves as a guide, assisting the attention module in prioritizing specific regions within the feature map. These regions hold the most valuable information for classifying traffic as benign or malicious. It combines the up sampled feature maps with the original, high-level features extracted by the encoder through skip connections. This ensures that the decoder retains both the broader context captured by the high-level features and the intricate details from the lower levels. This combination of high-level and low-level information is crucial for accurate intrusion detection in the complex and multifaceted world of IoT network traffic. The general representation for the attention mechanism is mathematically given in equation (5)

$$\overset{\square}{Data}_{i,Ch}^{la} = Data_{i,Ch}^{la} * \delta_i^{la} \tag{5}$$

Where $\overset{\square}{Data}_{i,Ch}^{la}$ signifies the Output of the attention module for channel ch at Traffic element i; $Data_{i,Ch}^{la}$ signifies the input feature map value for channel ch at Traffic element i; δ_i^{la} signifies the Attention coefficient for Traffic element i ranging from 0 to 1.

Classification layer:

Following the Attention Mechanism Integration, the LF-ACANet-GTOA model utilizes a fully connected layer for final intrusion detection. The fully connected layer assigns a probability score to each data point in the traffic data. These scores indicate the likelihood of the traffic being benign or belonging to a specific attack category. During the training phase, the proposed LF-ACANet-GTOA model leverages a cross-entropy loss function to evaluate its performance. This function calculates the difference between the predicted probabilities from the fully connected layer and the actual labels as benign or specific attack type in the training data. The general representation for the cross-entropy loss is mathematically represented in the following equation (6)

$$\text{Loss} = -\frac{1}{A}\sum_{j=1}^{A}\sum_{class=1}^{B}\left(y_{class,j}\right) * \ln\left(\overset{\square}{y}_{class,j}\right) \tag{6}$$

Where Loss depicts the calculated loss value for the model's prediction; A is Volume of training data; B depicts the Target variable cardinality (benign and different attack types). $y_{class,j}$ depicts the Ground truth label (1 for class $class$, 0 otherwise) for data point j; $\overset{\square}{y}_{class,j}$ depicts the predicted probability of data point j belonging to class $class$.

Optimizing for Accurate Intrusion Detection using GTOA

While the cross-entropy loss function evaluates the model's performance (Equation 5), minimizing this loss to achieve optimal intrusion detection requires a powerful optimization algorithm. For achieving this, Giant Trevally Optimization Algorithm (GTOA) was utilized. It mimics the hunting behaviour of giant trevally fish to iteratively search for the optimal configuration of weights and biases within the LF-ACANet model. This configuration minimizes the cross-entropy loss function, leading to improved Security monitoring solutions accuracy in Interconnected device networks. The flowchart of GTOA for minimizing the loss function of LF-ACANet model is given in the Figure 2. Below outlines the sequential procedure of GTOA,

Step 1: Initialization

Initially, GTOA starts by creating a random population of candidate solutions, represented as "trevallies." Each trevally corresponds to a possible configuration of weights and biases within the LF-ACANet model. These initial trevallies are scattered throughout the search space, ensuring exploration of various potential solutions. Each member of the population is mathematically represented by a vector, and it is given in equation (7)

$$S = \begin{bmatrix} S_1 \\ \vdots \\ S_p \\ \vdots \\ S_{Total} \end{bmatrix}_{Total \times Dim} \quad (7)$$

Where, S is the candidate solution (trevally); $Total$ is the number of trevallies (population size=25). $D\text{im}$ is the total number of weights and biases in the model. $S_{p,q}$ represents the value of the q^{th} variable in the p^{th} trevally.

Step 2: Random Position Assignment

Then, the initial positions of the trevallies are randomly established within the feasible search space, defined by the minimum and maximum values for each variable (weights and biases). It is given in equation (8)

$$S_{p,q} = Minimum_q + \left(Maximum_q - Minimum_q\right) * Random \quad (8)$$

Where $p = 1, 2........., Total$ and $q = 1, 2,........., Dim$; $Random$ is the probability distribution of the random variable is confined to the interval $\left(0,1\right)$.

Step 3: Fitness Function Evaluation

In this step, it evaluates the fitness function of each trevally using the Information divergence for classification (Equation 6). Estimates the cost of model inaccuracy between the LF-ACANet model's predictions (based on the current weights and biases of the trevally) and the actual labels (benign or attack type) in the training data. A lower loss value indicates better performance. It is given in equation (9)

$$Fitness\ Function\ (S) = Minimize[Loss] \quad (9)$$

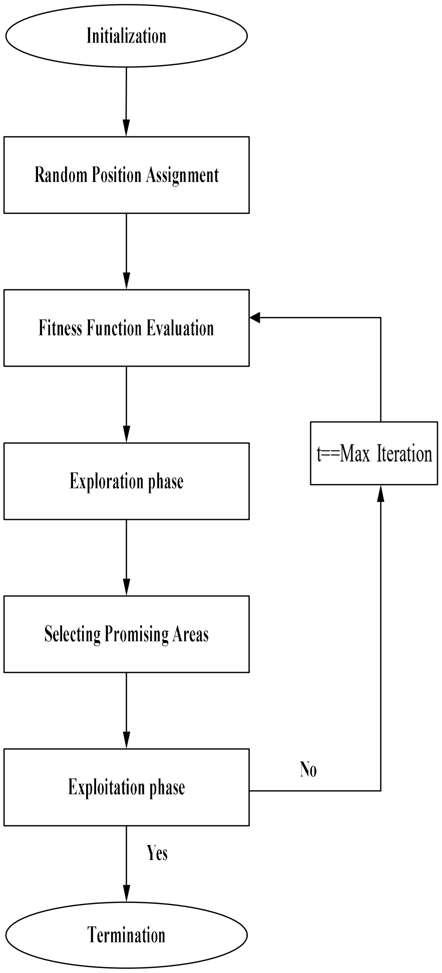

Figure 2: Flowchart of GTOA for optimizing the LF-ACANet model

Step 4: Exploration phase

Mimicking the long-distance foraging movements of trevallies, GTOA utilizes the Levy flight technique. This technique introduces random jumps into the search process, allowing trevallies to explore the entire solution space effectively [32]. By incorporating these jumps, GTOA avoids getting trapped in local minima. The Levy flight is described by equation (10),

$$S(t + 1) = Position_{Best} \times Random + \left((Maximum - Minimum) * R + Minimum\right) * Levy(Dim) \quad (10)$$

Here, $S(t+1)$ denotes the Spatial representation of the trevally in the subsequent iteration.; $Position_{Best}$ represents the current best position identified during the search; $Random$ is a random value within the range of 0 to 1; $Levy(Dim)$ demonstrates a search strategy inspired by Lévy flights.

Step 5: Selecting Promising Areas

As trevallies hunt for prey, they are drawn towards areas with abundant food sources. Similarly, GTOA leverages information from previous search iterations to guide the trevallies towards regions with potentially lower loss values. It considers both the best-performing solution found so far ($Position_{Best}$) and the average information ($Mean_{Info}$) across the trevallies in the population. This helps them focus their search on areas with potentially better solutions. This behaviour is mathematically represented by Equation (11)

$$S(t+1) = Position_{Best} \times A \times Random + Mean_{Info} - Si(t) \times Random \tag{11}$$

Where, A is a Movement amplitude parameter (usually within 0.3-0.4); $Si(t)$ is the giant trevally location i at current iteration t. $Mean_{Info}$ represents the average information from previous positions, calculated using Equation (12)

$$Mean_{Info} = \frac{1}{Total}\sum_{i=1}^{Total} Si(t) \tag{12}$$

Step 6: Exploitation phase

Once the trevallies have identified a promising area, they enter the exploitation phase. Here, they refine their positions around the best solution to converge towards an optimal configuration. This step simulates the attacking behaviour of giant trevallies, where they adjust their trajectory based on visual distortions caused by light refraction. GTOA incorporates this concept to guide the trevallies towards the solution with minimal loss i.e., potentially the most accurate intrusion detection configuration. The jumping function used in this stage is represented by Equation (13)

$$S(t+1) = \mathrm{LS} + \mathrm{VD} + \mathrm{JS} \tag{13}$$

Where VD represents the visual distortion, calculated using Equation (14)

$$\mathrm{VD} = \sin\left(\theta_1^{\circ}\right) \times \left|Position_{Best} - Si(t)\right| \tag{14}$$

Where $\sin\left(\theta_1^{\circ}\right)$ is calculated with the help of Snell's law and it is given by equation (15)

$$\sin\left(\theta_1^{\circ}\right) = \frac{\eta_2}{\eta_1} \times \sin\left(\theta_2^{\circ}\right) \tag{15}$$

Where Light propagation characteristics of air $\eta_1 = 1.00029$ and the Light propagation characteristics of water $\eta_2 = 1.33$; angle of incidence is represented as θ_1° and angle of refraction is represented as θ_2° and the values lies in the interval of $[0, 360]$. LS represents the launch speed, calculated using Equation (16)

$$\mathrm{LS} = \mathrm{Si(t)} \times \sin\left(\theta_2^{\circ}\right) \times Fitness\ Function\left(\mathrm{Si(t)}\right) \tag{16}$$

JS represents the jumping slope function (decreasing trend from 2 to 0), calculated using Equation (17),

$$\mathrm{JS} = \mathrm{Random} \times \left(2 - t \times \frac{2}{Max\ Iteration}\right) \tag{17}$$

Step 7: Termination

The entire process such as fitness evaluation, exploration, selection, and exploitation are repeated for a predefined number of iterations $(t == Max\ Iteration)$. With each iteration, the trevallies (candidate solutions) iteratively adjust their positions considering individual merit and group dynamics of other trevallies. This iterative process allows GTOA to gradually converge towards the optimal weights and biases that minimize the loss function, ultimately leading to the best possible intrusion detection performance for the LF-ACANet model.

The GTOA offers several advantages for optimizing the LF-ACANet loss function in intrusion detection. Firstly, it excels at effective search. By combining Levy flights for broad exploration and Selecting Promising Areas strategies to concentrate on promising regions with lower loss values, GTOA efficiently navigates the complex search space. Secondly, GTOA boasts improved convergence. The Exploitation phase refines a knowledge distillation approach, where past high-performing solutions guide the search process towards the optimal weight and bias configuration for the LF-ACANet model. Finally, Levy flights' inherent ability to take large jumps empowers GTOA to escape from local minima in the loss function. This translates to a more robust optimization process, ensuring the algorithm doesn't get stuck in suboptimal solutions and can effectively find the configuration that minimizes the loss function, leading to the most accurate intrusion detection performance.

By iteratively applying these steps, the GTOA algorithm helps the LF-ACANet model learn the appropriate weights and biases for effectively distinguishing between benign and malicious network traffic, achieving robust IoT intrusion detection.

4. OUTCOMES AND ANALYSIS

In this portion investigates the effectiveness of the LF-ACANet-GTOA Approach in bolstering IoT cybersecurity. The experiments took place on a on a setup featuring an Intel Core i7 processor (2.50 GHz), 8GB RAM, and running Windows 10. Python was the primary programming language for implementing the proposed LF-ACANet-GTOA model. The CIC-IDS-2017 and Bot-IoT datasets, established within the realm of IoT intrusion detection, were utilized for assessment. These datasets were segmented into three groups: training, validation, and assessment. The training set constitutes the largest portion of the data (60%). It's used to train the proposed LF-ACANet-GTOA model by exposing it to patterns and features for intrusion identification. The validation set comprises a smaller proportion compared to the training set (20%) and serves a crucial role in hyperparameter tuning. By adjusting hyperparameters based on validation set performance, the GTOA algorithm refines the LF-ACANet model's effectiveness. Finally, the testing set (20%) enabled the final evaluation of the LF-ACANet-GTOA model's performance. To comprehensively assess the proposed methodology, various evaluation metrics were considered. The analysis of these metrics yielded insights into the efficacy of the LF-ACANet-GTOA model. Furthermore, the results were compared with those achieved by existing methods in the proposed LF-ACANet-GTOA model compared with the existing methods like Imbalanced Security monitoring solutions in Interconnected device networks utilizing ensemble learning with deep neural networks (ELBC-DNN) [21], Decision Tree based resilient approach to detecting intrusions in Internet of Things networks (DT) [22] and Detecting Unknown Denial-of-Service Occurrences in Interconnected device networks with a SOCNN-LOF-iNNE Learning Model (SOCNN-LOF-iNNE) [23] respectively. This comparative analysis aimed to highlight the strengths and potential advantages of the proposed LF-ACANet-GTOA model.

Accuracy

Accuracy denotes the overall percentage of instances correctly classified. This is computed via following equation (18)

$$\text{Accuracy} = \frac{(\text{TP}+\text{TN})}{(\text{TP}+\text{FP}+\text{TN}+\text{FN})}$$

(18)

Where True Positive (TP): This pertains to the frequency of occasions when the model correctly identifies an attack, and the actual real-world activity was indeed an attack; True Negative (TN): This pertains to the frequency of occasions when the model correctly predicts normal activity, matching the actual real-world activity; False Positive (FP): This pertains to the frequency of occasions when the model correctly predicts normal activity, matching the actual real-world activity; False Negative (FN): This pertains to the frequency of occasions when the model correctly erroneously envisages normal activity, while the actual real-world activity was an attack.

Precision

It is the accuracy of the model's positive predictions (attacks). This is computed via following equation (19)

$$\text{Precision}=\frac{\text{TP}}{(\text{TP+FP})}$$

(19)

Recall

It measures the ratio of genuine attacks accurately identified as such by the model. This is scaled via equation (20)

$$\text{Recall}=\frac{\text{TP}}{(\text{TP+FN})} \tag{20}$$

F1 Score

A measure that strikes a balance the relationship of precision to recall. This is determined by equation (21)

$$\text{F1Score}=\frac{\text{TP}}{\left(\text{TP}+\frac{1}{2}[\text{FP+FN}]\right)} \tag{21}$$

False alarm rate

It calculates the fraction of negative predictions (normal activity) that the model erroneously classified as positive (attacks). This is computed with equation (22)

$$\text{False alarm rate} = 100 - \text{Precision} \tag{22}$$

Miss Rate

The Miss Rate represents the proportion of actual attacks that the model fails to identify. This is computed with equation (23)

$$\text{Miss rate} = 100 - \text{Recall} \tag{23}$$

4.1 Performance Analysis for CIC-IDS-2017 database

Figure 3-8 illustrate the working of a new intrusion detection system (IDS) called proposed LF-ACANet-GTOA method, evaluated using the CIC-IDS-2017 database. Figures 3-8 compare proposed LF-ACANet-GTOA against existing methods like ELBC-DNN [21], DT [22] and SOCNN-LOF-iNNE [23] across various cyberattacks.

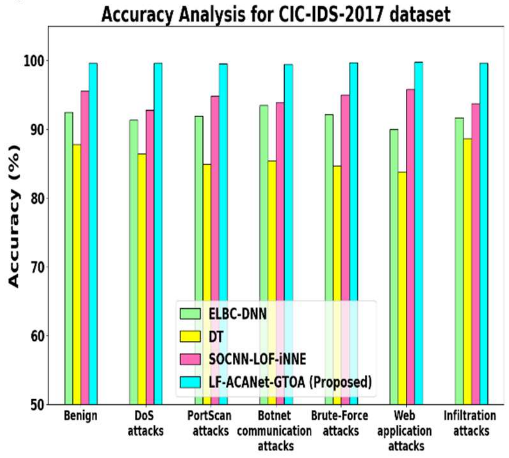

Figure 3: Accuracy representing CIC-IDS-2017

Figure 3 describes an analysis that compares accuracy achieved by assorted Security monitoring solutions (IDS) for a diverse range of cyberattacks within the CIC-IDS-2017 database. LF-ACANet-GTOA method attains 7.69%,13.41% and 4.18 high accuracy for Benign; 9.05%,15.24% and 7.36% high accuracy for Denial of Service attacks; 8.25%, 17.14% and 4.95% high accuracy for PortScan attacks; 6.34%, 16.45% and 5.86% high accuracy for Botnet communication attacks; 8.207%, 17.71% and 4.93% high accuracy for Brute-Force attacks; 10.801%,19.04% and 4.11% high accuracy for Web application attacks; 8.66%, 12.34% and 6.26% high accuracy for Infiltration attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively. The proposed LF-ACANet-GTOA method shows improvement in accuracy for various attack types compared to existing systems.

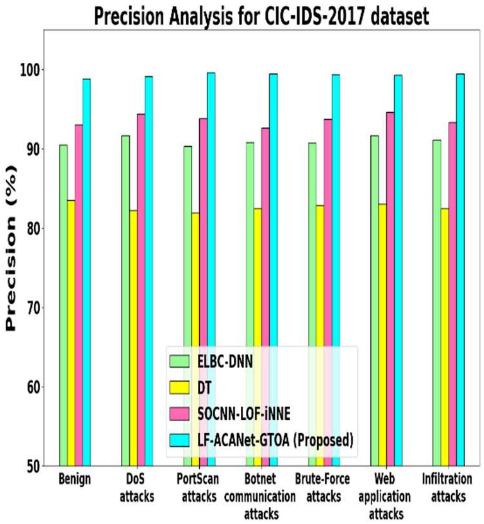

Figure 4: Precision representing CIC-IDS-2017

Figure 4 dives into the precision analysis of LF-ACANet-GTOA, showcasing its ability to identify true positives (correct malicious traffic) across various attack types in the CIC-IDS-2017. LF-ACANet-GTOA method attains 9.18%,18.34% and 6.216% high Precision for Benign; 8.15%,20.56% and 5.08% high Precision for Denial of Service attacks; 10.208%, 21.58% and 6.108% high Precision for PortScan attacks; 9.55%,20.59% and 7.38% high Precision for Botnet communication attacks; 9.58%,19.87% and 6.007% high Precision for Brute-Force attacks; 8.33%,19.61% and 5.002% high Precision for Web application attacks; 9.06%,20.56% and 6.55% high Precision for Infiltration attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively. Compared to existing me thods, the proposed LF-ACANet-GTOA method achieves significantly higher precision.

Figure 5 explores into the recall analysis of LF-ACANet-GTOA, focusing on its ability to detect all actual malicious traffic in the CIC-IDS-2017. LF-ACANet-GTOA method attains 7.22%, 13.91% and 4.29% high Recall for Benign; 8.53%, 16.84% and 6.15% high Recall for Denial of Service attacks; 8.74%, 18.56% and 8.098% high Recall for PortScan attacks; 8.51%, 19.76% and 6.706% high Recall for Botnet communication attacks; 9.93%, 21.79% and 9.05% high Recall for Brute-Force attacks; 8.68%, 20.99% and 7.81% high Recall for Web application attacks; 7.99%, 22.27% and 8.67% high Recall for Infiltration attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively. Compared to existing methods, proposed LF-ACANet-GTOA method demonstrates significant improvement in recall. This suggests it's more effective at catching these critical threats.

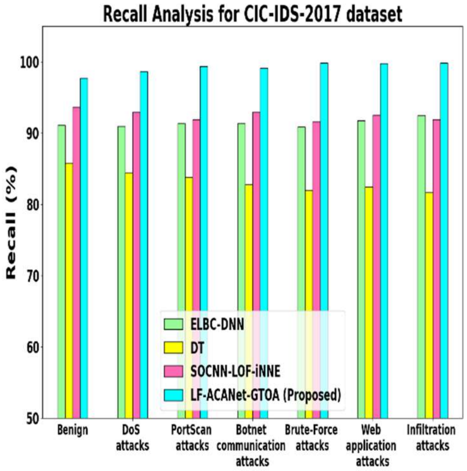

Figure 5: Recall representing CIC-IDS-2017

Figure 6 analyses the F-Score performance of the LF-ACANet-GTOA method on the CIC-IDS-2017. LF-ACANet-GTOA method attains 8.2%, 16.11% and 5.24% high F-Score for Benign; 8.34%, 18.701% and 5.623% high F-Score for Denial of Service attacks; 9.47%, 20.07% and 7.104% high F-Score for PortScan attacks; 9.03%, 20.18% and 7.04% high F-Score for Botnet communication attacks; 9.75%,20.83% and 7.52% high F-Score for Brute-Force attacks; 8.51%, 20.29% and 6.4% high F-Score for Web application attacks; 8.53%, 21.41% and 7.61% high F-Score for Infiltration attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively. Compared to existing methods, the proposed LF-ACANet-GTOA method achieves a significant overall improvement in F-Score across various attack types. This indicates a good balance between identifying true positives (malicious traffic) and minimizing false negatives (missed attacks) for these critical threats.

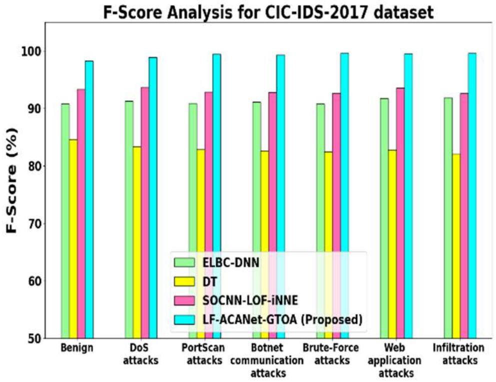

Figure 6: F-Score representing CIC-IDS-2017

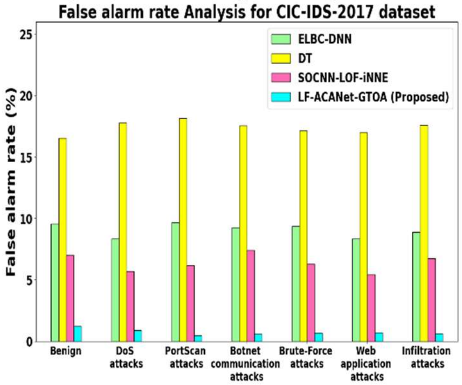

Figure 7: False alarm rate representing CIC-IDS-2017

Figure 7 showcases the strength of the proposed LF-ACANet-GTOA method in minimizing false alarms on the CIC-IDS-2017. False alarms occur when benign traffic is mistakenly identified as malicious. The proposed LF-ACANet-GTOA method attains 87.01%, 92.507% and 82.33% low False alarm rate for Benign; 89.46%, 95.05% and 84.507% low False alarm rate for Denial of Service attacks; 95.24%, 97.46% and 92.56% low False alarm rate for PortScan attacks; 93.83%, 96.75% and 92.307% low False alarm rate for Botnet communication attacks; 92.94%, 96.14% and 89.507% low False alarm rate for Brute-Force attacks; 91.49%, 95.82% and 86.94% low False alarm rate for Web application attacks; 93.01%, 96.47% and 90.78% low False alarm rate for Infiltration attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively. Compared to existing methods, the proposed LF-ACANet-GTOA method achieves significantly lower false alarm rates across all attack types. This translates to fewer unnecessary alerts and improved system efficiency.

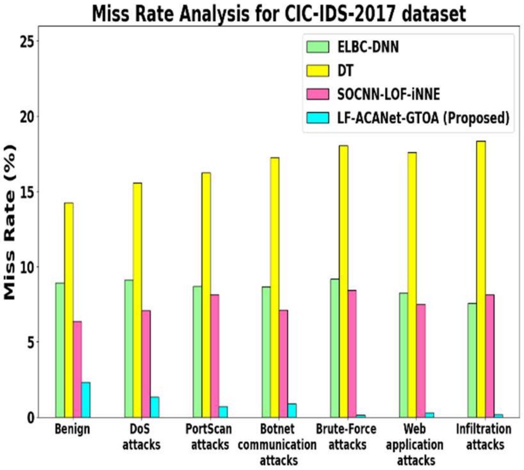

Figure 8: Miss rate Analysis for CIC-IDS-2017 dataset

Figure 8 depicts the Miss rate Analysis focusing on proposed LF-ACANet-GTOA's ability to catch actual malicious traffic and minimize missed attacks. This figure 8 showcases the method's strength, with consistently lower miss rates across all attack categories compared to existing methods. The proposed LF-ACANet-GTOA method attains 73.84%, 83.66% and 63.307% low Miss rate for Benign; 85.18%, 91.32% and 80.905% low Miss rate for Denial of Service attacks; 92.05%, 95.75% and 91.51% low Miss rate for PortScan attacks; 89.83%, 94.89% and 87.62% low Miss rate for Botnet communication attacks; 98.36%, 99.16% and 98.22% low Miss rate for Brute-Force attacks; 96.606%, 98.407% and 96.27% low Miss rate for Web application attacks; 97.88%, 99.12% and 98.03% low Miss rate for Infiltration attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively. However, the consistently low miss rates across various attack categories in Figure 8 strongly suggest proposed LF-ACANet-GTOA methods potential as a reliable intrusion detection system with a high success rate in catching malicious activity.

4.2 Analysing the performance on the Bot-IoT database:

Figure 9-14 illustrate the working of LF-ACANet-GTOA method for Bot-IoT dataset and Existing Methods like ELBC-DNN [21], DT [22] and SOCNN-LOF-iNNE [23] respectively.

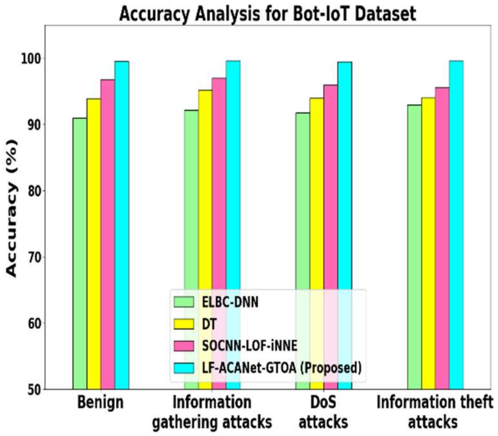

Figure 9: Accuracy representing Bot-IoT

Figure 9 illustrates the analysis of accuracy on the Bot-IoT. LF-ACANet-GTOA method attains 9.45%, 6.04% and 2.86% high accuracy for Benign; 8.12%, 4.708% and 2.69% high accuracy for Information gathering attacks; 8.45%, 5.87% and 3.65% high accuracy for Denial-of-Service attacks; 7.14%, 5.86% and 4.23% high accuracy for Information theft attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively.

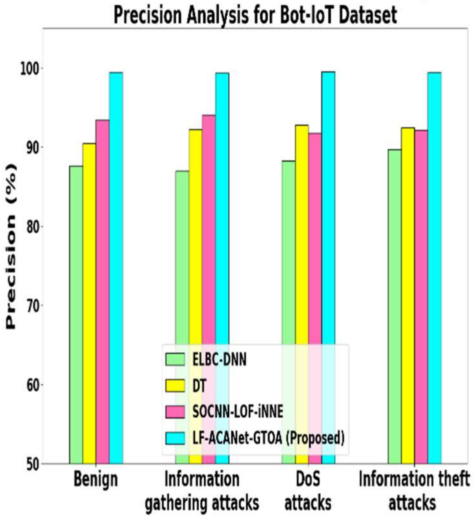

Figure 10: Precision representing Bot-IoT

Figure 10 illustrates the analysis of Precision on the Bot-IoT. LF-ACANet-GTOA method attains 13.43%, 9.92% and 6.39% high Precision for Benign; 14.25%, 7.77% and 5.63% high Precision for Information gathering attacks; 12.79%, 7.28% and 7.26% high Precision for Denial-of-Service attacks; 10.95%, 7.55% and 7.97% high Precision for Information theft attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively.

Figure 11 illustrates the analysis of Recall on the Bot-IoT. LF-ACANet-GTOA method attains 15.11%, 10.27% and 6.35% high Recall for Benign; 13.69%, 8.92% and 6.81% high Recall for Information gathering attacks; 13.06%, 8.54% and 5.74% high Recall for Denial-of-Service attacks; 12.31%, 7.54% and 7.29% high Recall for Information theft attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively.

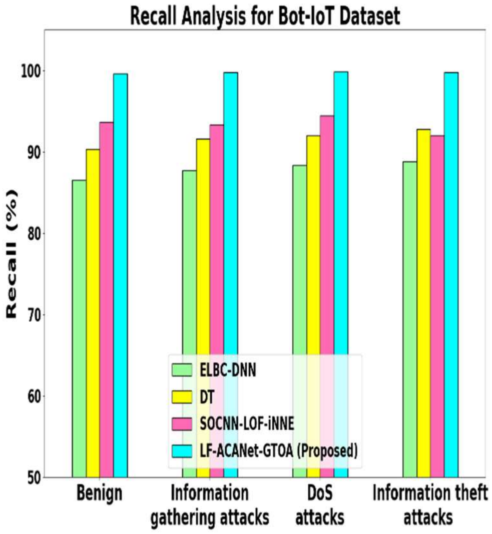

Figure 11: Recall representing Bot-IoT

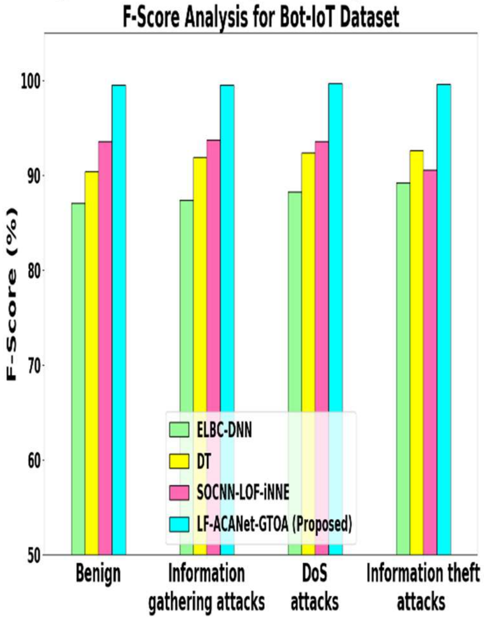

Figure 12: F-Score representing Bot-IoT

Figure 12 illustrates the analysis of F-Score on the Bot-IoT. LF-ACANet-GTOA method attains 14.27%, 10.1% and 6.37% high F-Score for Benign; 13.97%, 8.34% and 6.22% high F-Score for Information gathering attacks; 12.92%, 7.91% and 6.508% high F-Score for Denial-of-Service attacks; 11.63%, 7.55% and 7.63% high F-Score for Information theft attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively.

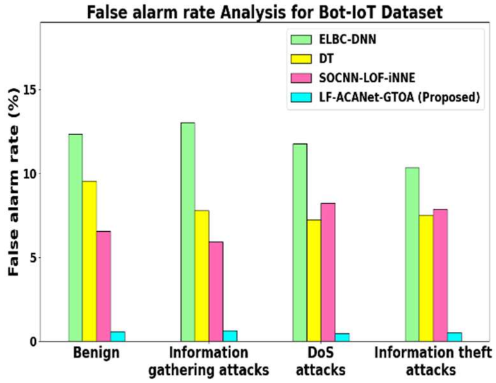

Figure 13: False alarm rate representing Bot-IoT

Figure 13 illustrates the analysis of False alarm rate on the Bot-IoT. LF-ACANet-GTOA method attains 95.38%, 94.03% and 91.29% low False alarm rate for Benign; 95.23%, 92.04% and 89.52% low False alarm rate for Information gathering attacks; 95.92%, 93.37% and 93.35% low False alarm rate for Denial-of-Service attacks; 94.87%, 92.95% and 93.27% low False alarm rate for Information theft attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively.

Figure 14 illustrates the analysis of Miss rate on the Bot-IoT. LF-ACANet-GTOA method attains 97.17%, 96.06% and 93.99% low Miss rate for Benign; 97.801%, 96.8% and 95.92% low Miss rate for Information gathering attacks; 98.97%, 98.49% and 97.83% low Miss rate for Denial-of-Service attacks; 97.85%, 96.68% and 96.58% low Miss rate for Information theft attacks compared with the existing methods like ELBC-DNN, DT and SOCNN-LOF-iNNE respectively.

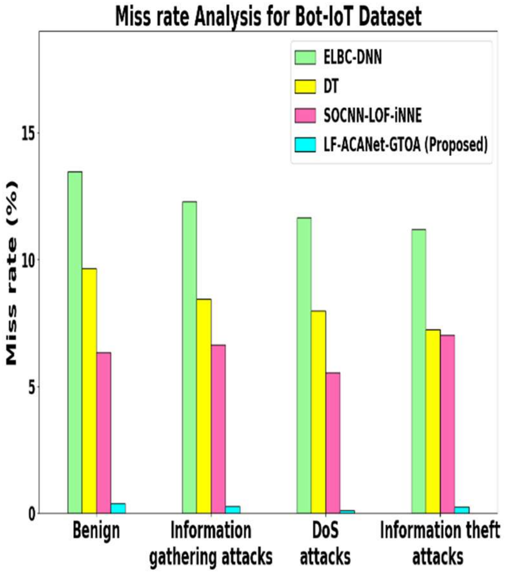

Figure 14: Miss rate representing Bot-IoT

4.3 Discussion

In this part, it analyses the effectiveness of the LF-ACANet-GTOA Security monitoring solutions (IDS) on two datasets: CIC-IDS-2017 and Bot-IoT. The comparison estimates the effectiveness of the LF-ACANet-GTOA method's measures against existing methods like ELBC-DNN, DT, and SOCNN-LOF-iNNE for various cyberattacks.

The proposed LF-ACANet-GTOA method consistently achieved higher accuracy in identifying various cyberattacks compared to existing methods. This indicates its effectiveness in correctly classifying both benign and malicious traffic. It also demonstrated a good balance between identifying malicious traffic and minimizing benign traffic flagged as malicious. This translates to fewer unnecessary alerts and improved system efficiency. Compared to existing methods, proposed LF-ACANet-GTOA method achieved substantially lower miss rates for both benign and malicious traffic. This signifies its improved ability to catch a wider range of threats while minimizing missed detections.

While proposed LF-ACANet-GTOA method demonstrates promising results, there are areas for improvement. Evaluating it on more datasets and investigating scalability for larger networks are crucial next steps. Additionally, incorporating explainability techniques can improve understanding of its decision-making process. Future work can explore integrating blockchain technology with LF-ACANet-GTOA to bolster IDS security in IoT. Blockchain offers a secure and tamper-proof platform to store statistics employed for guidance and assessment the model, enhancing statistics integrity and trustworthiness. Furthermore, leveraging blockchain's immutability and distributed ledger technology can significantly strengthen the overall security of the IDS in IoT networks.

5. CONCLUSION

In this section, the proposed Lightweight Fortified Attentional Convolutional Network with Giant Trevally Optimization Algorithm (LF-ACANet-GTOA) demonstrates significant potential for securing resource-constrained Internet of Things (IoT) networks. This meticulously designed system tackles intrusion detection challenges effectively. The pre-processing phase ensures clean data for the model, while the unique architecture with convolutional encoders, Feature Enrichment Block, Attention Mechanism Integration, and classification layers efficiently extracts features and classifies the intrusion. Additionally, the Giant Trevally Optimization Algorithm (GTOA) optimizes the model's performance. Analysis on benchmark datasets reveals superior accuracy, balanced detection with minimized false alarms, and reduced miss rates compared to existing methods. While promising, further evaluation on diverse datasets and scalability investigations are necessary. Additionally, incorporating explainability techniques can improve comprehension of the process of decision-making. Future work can explore integrating blockchain technology to enhance data integrity, immutability, and overall security of the Security monitoring solutions in Interconnected device networks. By continuously refining LF-ACANet-GTOA and exploring promising avenues like blockchain integration, a robust and secure future for Security monitoring solutions in Interconnected device networks can be created.

Compliance with Ethical Standards

Conflict of interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Informed Consent

Informed consent does not apply as this was a retrospective review with no identifying patient information.

Funding: Not applicable

Conflicts of interest Statement: Not applicable

Consent to participate: Not applicable

Consent for publication: Not applicable

Availability of data and material:

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Code availability: Not applicable

Competing Interests: Not applicable

REFERENCES

[1] Otoum, Y., Liu, D. and Nayak, A., 2022. DL-IDS: a deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 33(3), p.e3803.

[2] Alghamdi, R. and Bellaiche, M., 2023. An ensemble deep learning based IDS for IoT using Lambda architecture. Cybersecurity, 6(1), p.5.

[3] Ahad, U., Singh, Y., Anand, P., Sheikh, Z.A. and Singh, P.K., 2022. Intrusion detection system model for IoT networks using ensemble learning. Journal of Interconnection Networks, 22(03), p.2145008.

[4] Saheed, Y.K., 2022. Performance improvement of intrusion detection system for detecting attacks on internet of things and edge of things. In Artificial Intelligence for Cloud and Edge Computing (pp. 321-339). Cham: Springer International Publishing.

[5] Aldhaheri, A., Alwahedi, F., Ferrag, M.A. and Battah, A., 2023. Deep learning for cyber threat detection in IoT networks: A review. Internet of Things and Cyber-Physical Systems.

[6] Gorzałczany, M.B. and Rudziński, F., 2022. Intrusion Detection in Internet of Things With MQTT Protocol—An Accurate and Interpretable Genetic-Fuzzy Rule-Based Solution. IEEE Internet of Things Journal, 9(24), pp.24843-24855.

[7] Ioannou, I., Nagaradjane, P., Angin, P., Balasubramanian, P., Kavitha, K.J., Murugan, P. and Vassiliou, V., 2024. GEMLIDS-MIOT: A Green Effective Machine Learning Intrusion Detection System based on Federated Learning for

Medical IoT network security hardening. Computer Communications.

[8] Campos, E.M., Saura, P.F., González-Vidal, A., Hernández-Ramos, J.L., Bernabe, J.B., Baldini, G. and Skarmeta, A., 2022. Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks, 203, p.108661.

[9] Samriya, J.K., Tiwari, R., Cheng, X., Singh, R.K., Shankar, A. and Kumar, M., 2022. Network intrusion detection using ACO-DNN model with DVFS based energy optimization in cloud framework. Sustainable Computing: Informatics and Systems, 35, p.100746.

[10] Stiawan, D., Idris, M.Y. and Budiarto, R., 2022. Impact of Dimensionality Reduction on Performance of IoT Intrusion Detection System. In Internet of Things (pp. 101-124). CRC Press.

[11] Aljebreen, M., Mengash, H.A., Arasi, M.A., Aljameel, S.S., Salama, A.S. and Hamza, M.A., 2023. Enhancing DDoS attack detection using snake optimizer with ensemble learning on internet of things environment. IEEE Access.

[12] Arshad, K., Ali, R.F., Muneer, A., Aziz, I.A., Naseer, S., Khan, N.S. and Taib, S.M., 2022. Deep reinforcement learning for anomaly detection: A systematic review. IEEE Access, 10, pp.124017-124035.

[13] Chauhan, A., Saini, S., Sapra, L. and Thakur, G., 2022. Intrusion Detection Systems Apropos of the Internet of Things (IoT). In Internet of Things and Cyber Physical Systems (pp. 167-182). CRC Press.

[14] Heidari, A. and Jabraeil Jamali, M.A., 2023. Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Computing, 26(6), pp.3753-3780.

[15] Adawadkar, A.M.K. and Kulkarni, N., 2022. Cyber-security and reinforcement learning—A brief survey. Engineering Applications of Artificial Intelligence, 114, p.105116.

[16] Gorzałczany, M.B. and Rudziński, F., 2022. Intrusion Detection in Internet of Things With MQTT Protocol—An Accurate and Interpretable Genetic-Fuzzy Rule-Based Solution. IEEE Internet of Things Journal, 9(24), pp.24843-24855.

[17] Hairab, B.I., Elsayed, M.S., Jurcut, A.D. and Azer, M.A., 2022. Anomaly detection based on CNN and regularization techniques against zero-day attacks in IoT networks. IEEE Access, 10, pp.98427-98440.

[18] Ramachandran, P. and Balasubramian, R., 2022. An Automatic Correlated Recursive Wrapper-Based Feature Selector (ACRWFS) for Efficient Classification of Network Intrusion Features. In Intelligent Sustainable Systems: Proceedings of ICISS 2021 (pp. 647-660). Springer Singapore.

[19] Aydın, H., Aydın, G.Z.G., Sertbaş, A. and Aydın, M.A., 2023. Internet of things security: A multi-agent-based defense system design. Computers and Electrical Engineering, 111, p.108961.

[20] De Keersmaeker, F., Cao, Y., Ndonda, G.K. and Sadre, R., 2023. A survey of public IoT datasets for network security research. IEEE Communications Surveys & Tutorials.

[21] Thakkar, A. and Lohiya, R., 2023. Attack classification of imbalanced intrusion data for IoT network using ensemble learning-based deep neural network. IEEE Internet of Things Journal.

[22] Nguyen, D.T. and Le, K.H., 2023. The robust scheme for intrusion detection system in internet of things. Internet of Things, 24, p.100999.

[23] Nguyen, X.H. and Le, K.H., 2023. Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model. Internet of Things, 23, p.100851.

[24] Bakhsh, S.A., Khan, M.A., Ahmed, F., Alshehri, M.S., Ali, H. and Ahmad, J., 2023. Enhancing IoT network security through deep learning-powered Intrusion Detection System. Internet of Things, 24, p.100936.

[25] Li, S., Cao, Y., Liu, S., Lai, Y., Zhu, Y. and Ahmad, N., 2024. HDA-IDS: A Hybrid DoS Attacks Intrusion Detection System for IoT by using semi-supervised CL-GAN. Expert Systems with Applications, 238, p.122198.

[26] Vishwakarma, M. and Kesswani, N., 2023. A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection. Decision Analytics Journal, 7, p.100233.

[27] Saheed, Y.K., Abiodun, A.I., Misra, S., Holone, M.K. and Colomo-Palacios, R., 2022. A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), pp.9395-9409.

[28] CIC-IDS-2017 Dataset: https://www.unb.ca/cic/datasets/ids-2017.html.

[29] Bot-IoT Dataset: https://research.unsw.edu.au/projects/bot-iot-dataset.

[30] Dash, C.S.K., Behera, A.K., Dehuri, S. and Ghosh, A., 2023. An outliers detection and elimination framework in classification task of data mining. Decision Analytics Journal, 6, p.100164.

[31] Munir, F., Azam, S., Jeon, M., Lee, B.G. and Pedrycz, W., 2021. LDNet: End-to-end lane marking detection approach using a dynamic vision sensor. IEEE Transactions on Intelligent Transportation Systems, 23(7), pp.9318-9334.

[32] Sadeeq, H.T. and Abdulazeez, A.M., 2022. Giant trevally optimizer (GTO): A novel metaheuristic algorithm for global optimization and challenging engineering problems. Ieee Access, 10, pp.121615-121640.