International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 8, Issue 3, May-June 2025||

DOI:10.15662/IJRAI.2025.0803010

AI Based Cybersecurity for Internet of Things Networks via Self-Attention Deep Learning and Metaheuristic Algorithms

Pavan Navandar

Cyber Security Architect & Lead, USA

ABSTRACT: Recently, Internet of Things (IoT) usage has increased rapidly, and cybersecurity concerns have also improved. Cybersecurity attacks are exclusive to the IoT, which has unique limitations and characteristics. Considering that many attacks and threats are being presented daily against IoT. So, it is significant to recognize these kinds of attacks and discover solutions to alleviate their risks. The modern approach to cybersecurity comprises the application of artificial intelligence (AI) to develop complex models for protecting systems and networks, specifically in IoT environments. Cyber attackers have also adapted by leveraging AI technologies, using adversarial AI to execute advanced cybersecurity threats. This constant evolution of AI-driven threats and defenses necessitates developing more robust, adaptive, and real-time cybersecurity models to stay ahead of increasingly advanced attacks. This paper presents an Intelligent Cybersecurity System Using Self-Attention-based

Deep Learning and Metaheuristic Optimization Algorithm (ICSSADL-MHOA). The proposed ICSSADLMHOA model aims to enhance a robust cybersecurity system in IoT networks. At first, the data normalization stage employs min–max normalization to ensure consistency, accuracy, and efficiency by organizing data into a standardized format. Furthermore, the improved tuna swarm optimization (ITSO) model is implemented for the feature selection process to detect the most relevant features in the data. Besides, the proposed ICSSADL-MHOA model utilizes the bidirectional long short-term memory with self-attention (BiLSTM-SA) model for the detection and classification method of cybersecurity. Finally, the parameter selection of the BiLSTM-SA technique is performed by employing the hunger games search (HGS) technique. Comprehensive studies under the ToN-IoT and Edge-IIoT datasets validate the efficiency of the ICSSADL-MHOA method. The experimental validation of the ICSSADL-MHOA method illustrated a superior accuracy value of 99.37% over existing techniques.

KEYWORDS: Cybersecurity, IoT, Tuna Swarm Optimization, Hyperparameter Selection, Attacks, Data Normalization

I. INTRODUCTION

Due to rising demand and the growth of innovative network systems of IoTs. However, its concepts have become more complex day by day. IoT is demanding to describe because it has improved and evolved since it was primarily developed[1]. Even the best definition describes it as a connected digital network where devices with unique UIDs can swap data autonomously without human intervention[2]. It is often deliberated as a user interface for a centralized or system location application, usually a smartphone application that sends instructions or data to more than single-edge IoT gadgets. IoT gadgets are susceptible to Internet threats due to several attack vectors[3]. Hackers might exploit cybersecurity vulnerabilities in IoT devices, which depend upon the specific part of their target network, leading to different threats. IoT-related cyber security studies are very active right now. Cybersecurity might be significantly assisted by AI[4]. Cyber security is implicated in safeguarding software, data, and electronics, together with the processes by which methods are acquired[5]. Generally, security intentions include privacy regarding information adequately disclosed to unauthorized gadgets or people to be destroyed or modified. Consequently, owing to limitless IoT-based connected gadgets, society is also becoming gradually susceptible to cyberthreats like denial-of-service (DoS) threats by insiders and hackers[6]. Technology is progressively more important in everyday existence, which means cybersecurity and cybercrime devices progress simultaneously through the whole manufacturing area, which requires investing in cybersecurity countermeasures. In contrast, innovative technologies have been developed for IoT cybersecurity management. Additionally, cyber-threats on smart grids, as primary structural elements, are mainly susceptible and bear more costs, and they rigorously affect the safety of governments and citizens[7]. There is an increasing interest in cyber security and the absence of effectual countermeasures, for example, cyber security experts. Figure 1 signifies the common architecture of cybersecurity in IoT devices.

Because of their better performance in a range of prediction-based domains, in recent times, investigators have aimed at machine learning (ML) and deep learning (DL) models. Using AI models like DL and ML methodology might provide effective approaches to data usage to identify and predict possible cybersecurity attacks. DL approaches recognize cyber threats that are increasingly popular more quickly than preceding models that allow more effective mitigation[8]. DL is a subdivision of AI that focuses on handling and calculating machine applications, which can be complicated, non-linear designs, and then employing those designs to make predictions. In the cybersecurity world, DL techniques have become gradually popular devices, rapidly vital to effective defence approaches against harmful attacks. Since IoT gadgets have become more connected, the possibility of hacks has improved. The rapid expansion of IoT devices has significantly enhanced the complexity of cybersecurity challenges, creating new vulnerabilities that cybercriminals exploit[9]. As IoT systems become more integrated into everyday life, ensuring their security is significant to prevent unauthorized access and malicious attacks. The interconnected behaviour of these devices makes them a prime target for cyber threats, necessitating advanced security measures. Conventional methods are often insufficient, highlighting the need for more innovative solutions that address these growing risks. Leveraging artificial intelligence and advanced algorithms is becoming crucial to improve the protection and resilience of IoT networks[10].

This paper presents an Intelligent Cybersecurity System Using Self-Attention-based Deep Learning and Metaheuristic Optimization Algorithm (ICSSADL-MHOA). The proposed ICSSADL-MHOA model aims to enhance a robust cybersecurity system in IoT networks. At first, the data normalization stage employs min– max normalization to ensure consistency, accuracy, and efficiency by organizing data into a standardized format. Furthermore, the improved tuna swarm optimization (ITSO) model is implemented for the feature selection process to detect the most relevant features in the data. Besides, the proposed ICSSADL-MHOA model utilizes the bidirectional long short-term memory with self-attention (BiLSTM-SA) model for the detection and classification method of cybersecurity. Finally, the parameter selection of the BiLSTM-SA technique is performed by employing the hunger games search (HGS) technique. Comprehensive studies under the ToNIoT and Edge-IIoT datasets validate the efficiency of the ICSSADL-MHOA method. The key contribution of the ICSSADL-MHOA method is listed below.

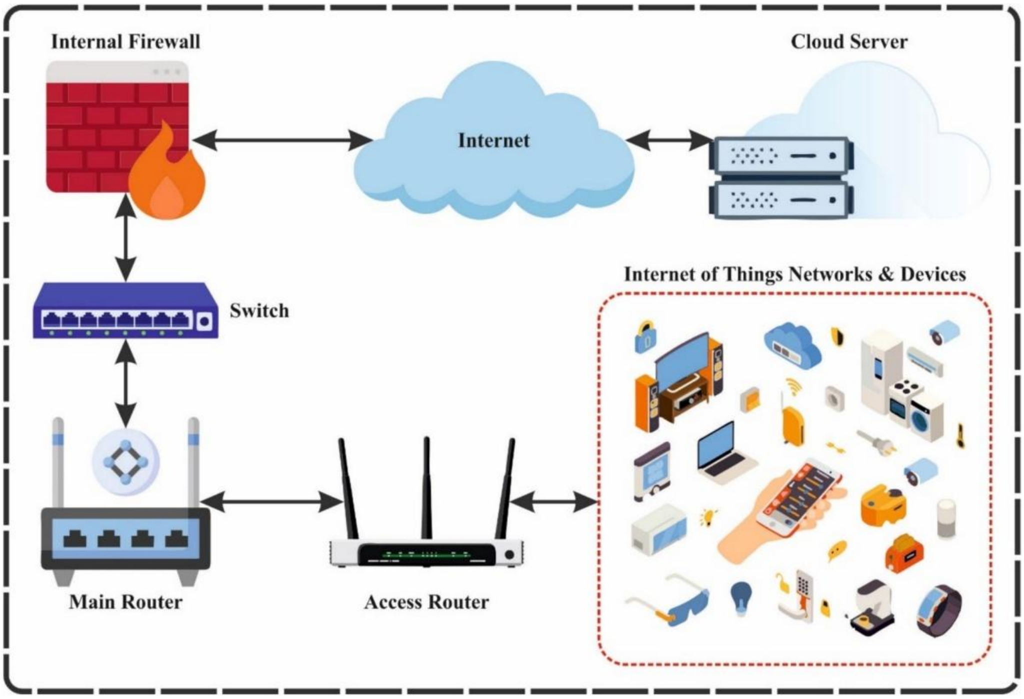


Fig. 1: General structure of cybersecurity in IoT networks.

- The ICSSADL-MHOA model utilizes min–max normalization to scale features within a consistent range, improving input uniformity. This approach enhances the stability of the model and ensures improved performance by preventing the dominance of larger values. By normalizing the data, the model effectively handles varying feature scales, resulting in more accurate results.
- The ICSSADL-MHOA method employs the ITSO approach for feature selection, detecting the most important features for the task. This methodology improves classification accuracy by mitigating irrelevant features, allowing the model to concentrate on the most impactful data. ITSO assists in achieving optimal feature subsets, improving the overall efficiency of the model.
- The ICSSADL-MHOA approach utilizes the BiLSTM model incorporated with SA to capture past and future context in data sequences. Concentrating on relevant patterns in the data significantly enhances the model's capability to detect and classify cybersecurity threats. The model improves its predictive accuracy and threat detection robustness by integrating temporal and contextual data.
- The ICSSADL-MHOA methodology employs the HGS approach to optimize the selection of model parameters, improving its capability to converge efficiently. By fine-tuning parameters, the technique enhances the overall performance of the model. This approach confirms that the model reaches optimal solutions, improving accuracy and computational efficiency.
- The ICSSADL-MHOA method integrates ITSO for feature selection, BiLSTM-SA for detection and classification, and HGS for parameter optimization, giving a comprehensive and efficient solution. This multi-algorithmic approach improves the accuracy and robustness of the model in cybersecurity tasks. The novelty is in the seamless integration of optimization, DL, and feature selection techniques, creating a highly effective framework tailored for IoT environments. This integration confirms superior threat detection and resource optimization in complex cybersecurity scenarios.

The article is structured as follows: Sect. "Literature Survey" presents the literature review, Sect. "Materials and Methods" outlines the proposed method, Sect. "Experimental Validation and Discussion" details the results evaluation, and Sect. "Conclusion" concludes the study.

II. LITERATURE SURVEY

Imtiaz et al.[11]developed XIoT, an innovative XIoT threat recognition method to address these challenges. Exploiting sophisticated DL approaches, particularly Convolutional Neural Network (CNN), XIoT examines spectrogram images changed to IoT system traffic information to identify subtle and complex threat patterns. Unlike conventional methods, XIoT highlights interpretability by incorporating CNNs, Explainable AI (XAI) methods, allowing cyber security analysts to trust and understand its forecasts. Additionally, these technique structures utilize the lower-latency, higher-speed optical network features. In[12], a DL-based structure is developed with multiple optimizations for automatically classifying and detecting cyber threats. These optimizations contain hyper-parameter tuning, feature engineering, and reduction of dimensions. Sattarpour et al.[13] developed an innovative anomaly-based IDS exploiting DL models, mainly aimed at the Bidirectional Encoder Representations from Transformers (BERT) model. BERT's structure allows it to implement lesser cost evaluations and recognitions than other advanced models, making it appropriate for resource-constrained IoT settings. The developed structure, EBIDS, connects the ability of BERT to improve intrusion detection (ID) at the network or IoT systems. Morshedi et al.[14] developed an innovative IoT network ID (NID) method, exploiting DL models and pristine data. The aim is to give a more efficient model than the preceding models. The developed DL technique integrates LSTM structure and densely transition layers, intending to take spatial or temporal dependency in the data. Ragab et al.[15] intend a Next-Generation Cybersecurity Attack Detection employing an ensemble DL model (NGCAD-EDLM) methodology in IIoT settings. Moreover, an ensemble DL of dual models, such as deep belief network (DBN) and CNN approaches, are applied for classification. Furthermore, the DL model's hyper-parameter choice is achieved using the lotus effect optimizer algorithm (LEOA) approach. Alsoufi et al.[16] enhance and design a new anomaly-based ID system (AIDS) for IoT systems. Primarily, an SAE is utilized to minimize the higher dimension and acquire substantial data representation by determining the rebuilt error. Afterwards, the CNN model was used to generate a dual classification method. Al-Neami et al.[17]developed an innovative method to enlarge the Field-Programmable Gate Array (FPGA) to enlarge a higher-performance IDS. The presented method incorporates advanced models containing Extreme Gradient Boosting (XGBoost), Hybrid DL (HDL) model, and Meta Ensemble Learning (MEL) that relate LSTM methods for temporal investigation and CNN for extracting features. This synergistic method substantially decreases detection latency and increases the threat recognition precision. Wang, Dai, and Yang[18] developed a NID model based on DL. Also, a Conditional Tabular Generative Adversarial Network (CTGAN) generates synthetic data for the minority class.

Generative Adversarial Network (SAPGAN) with Namib Beetle Optimization Algorithm (NBOA). It integrates data pre-processing with APPDRC, feature selection via WSOA, and intrusion classification for diverse attacks. NBOA optimizes SAPGAN's parameters for improved attack classification accuracy. Tewari and Gupta[20] analyze and address the security challenges in IoT across its three layers, namely perception, transportation, and application, exploring cross-layer integration issues and comparing them with conventional network security problems. Aboalela et al.[21]introduce the Harnessing Feature Pruning with Optimal DL DDoS Cyberattack Detection (HFPODL-DDoSCD) approach for effectual DDoS attack detection in IoT environments. It uses Z-score normalization, Siberian Tiger Optimization (STO) for feature selection, and an SA-BiTCN-BiGRU model for attack detection. Parameter tuning is performed using the Artificial Protozoa Optimizer (APO) to optimize performance. Adat and Gupta[22] analyze the security threats in IoT, provide a taxonomy of security issues and defence mechanisms, and discuss future research directions to address existing gaps and improve IoT security. Santhanamari et al.[23]propose a robust security framework using the Cosine CNN (CCNN) technique for attack detection, improving feature extraction with cosine similarity. The Exponential Distribution Optimizer (EDO) optimizes CCNN, balancing exploration and exploitation for optimal performance. Zhao, Li, and Li[24] propose a secure authentication scheme incorporating semantic LSTM and blockchain (BC) to improve authentication, access control, and security in IoT applications while reducing computational overhead. Wang et al.[25] propose a deep residual SConv1D-Attention model. The method utilizes binary Particle Swarm Optimization (bPSO) for feature selection, a novel SConv1D-Attention module for effectual information integration, and a robust loss function for addressing data imbalance by accentuating minority classes. Reka et al.[26] present a Centrality Coati Optimization Algorithm (COA)-based Cluster Gradient for multi-attack intrusion identification in MANETs. It utilizes Dual Network Centrality for cluster head selection and the COA for compact clustering. The Multi-head Self-Attention based Gated Graph Convolutional Network (MSA-GCNN) detects various attacks. Mohamed et al.[27] introduced a probabilistic composite model for zero-day exploit detection. It features Adaptive WavePCA-Autoencoder (AWPA) for denoising and dimensionality reduction (DR), Meta-Attention Transformer Autoencoder (MATA) for improved feature extraction, Genetic Mongoose-Chameleon Optimization (GMCO) for efficient feature selection, and Adaptive Hybrid Exploit Detection Network (AHEDNet) for dynamic ensemble adaptation, achieving high accuracy and low false positives.

Ashwini and Nagasundara[28] propose the Enhanced Dual Vision Transformer (EDVT) integrated with the Mantis Search Split Attention Network (MSSAN) models for ransomware detection and classification. It utilizes the log-sinh with Adaptive Box-Cox Transformation (log-sinhABT) for data pre-processing and the Hybrid Termite Alate City Council's Evolution Optimization (HTCEO) for efficient feature selection. Zareh Farkhady et al.[29] present a three-dimensional DL (3DLBS) approach for attack detection, transforming 1D data into 3D using shape, fill, and permute techniques. The model also utilizes CNN and LSTM branches for detection and uses binary chimp optimization (BCHO) for feature selection, improving accuracy and speed. Perumal et al.[30]propose the Enhanced Metaheuristics with DL Model for BC Assisted Cybersecurity Solution (EMDLM-BCCS) technique. It uses data pre-processing, extreme learning machine (ELM) for attack detection, and elite-oppositional grasshopper optimization (EGOA) to enhance ELM performance. Orman[31] proposes an IDS framework integrating Multi-layer Perceptron (MLP), ML, DL, Random Forest (RF), and hybrid models. Kocherla et al.[32]introduce the DLAD model, a bio-inspired metaheuristic for anomaly detection in IIoT.

The technique also utilizes the Improved Crow Search Algorithm (ICSA) method for feature selection, Stacked Recurrent Neural Networks (SRNN) and Harris Hawks Optimizer (HHO) techniques for classification and parameter tuning. Alqahtany, Shaikh, and Alqazzaz[33]introduce an IDS using Enhanced Grey Wolf Optimization (EGWO) methodology for feature selection to improve reliability and computational efficiency in IoT networks. Babitha[34]develops a quantum-inspired BC-assisted cybersecurity model for IoT, utilizing the Fitness-based Jellyfish Chameleon Swarm Algorithm (FJCSA) technique for key optimization and Adaptive Attention-based LSTM with Adaboost (AALSTM-Ab) model for ID. Anu Velavan and Sureshkumar[35] propose a Double Fuzzy Clustering-Driven Context Neural Network for ID in Cloud Computing (DFCCNN-BWOA-IDC) model for ID in cloud computing. The method also employs Sequential pre-processing for data cleaning, Recursive Feature Elimination (RFE) for feature selection, and the Beluga Whale Optimization (BWO) approach to optimize DFCCNN parameters for accurate attack detection. Lakicevic et al.[36]propose a phishing email detection methodology by employing an artificial neural networks (ANN) model with soft attention and BERT encoders optimized by a modified crayfish optimization algorithm (COA) method to improve classification accuracy. Sayeed, Ahmed, and Swamy[37]present a multimodal biometric system utilizing palm and knuckle vein recognition. The technique also employs contrast enhancement for pre-processing, GLCM and DWT for feature extraction, Chimp Optimization Algorithm (ChOA) technique for feature selection, and a Deep Neural Network (DNN) model for classification. Althobaiti and Escorcia-Gutierrez[38] introduce the weighted salp swarm algorithm with DL-based cyber-threat detection and classification (WSSADL-CTDC) technique for cyber-threat detection, incorporating a weighted salp swarm algorithm, DL, and min–max normalization. The method utilizes the shuffled frog leap algorithm (SFLA) for feature selection and a hybrid convolutional autoencoder (CAE) model with WSSA-based hyperparameter tuning for improved performance. Table 1 summarizes the existing studies on AI-based cybersecurity systems.

Despite the significant improvements in IoT security solutions, various limitations remain. Many existing methods depend heavily on specific optimization algorithms or models that may not generalize well across diverse IoT environments, such as XIoT, EBIDS, SAPGAN, etc. The reliance on high computational resources in specific approaches limits their scalability for resource-constrained IoT devices. Additionally, various methodologies suffer from challenges in feature selection and the handling of imbalanced data, such as HFPODL-DDoSCD and SConv1D-Attention, which affect their accuracy in detecting minority class threats. Furthermore, most current models do not sufficiently address cross-layer security issues in IoT, leaving gaps in comprehensive protection strategies. Lastly, there is a requirement for more efficient and low-latency techniques to address real-time ID in IoT systems, as highlighted by the proposed methods in several studies like IDS-SAPGAN and EDVT. A significant research gap is the requirement for more dynamic and context-aware security mechanisms that adapt to the evolving nature of IoT environments and growing threats.

III. MATERIALS AND METHODS

This paper presents a novel ICSSADL-MHOA technique. The proposed ICSSADL-MHOA model aims to enhance a robust cybersecurity system in IoT networks. It involves various processes, such as data normalization, DR, classification, and parameter tuning. Figure 2 signifies the complete work procedure of the ICSSADL-MHOA model.

Ref.No	Objective	Method	Dataset	Measures
11	To develop XIoT, an explainable IoT attack detection model using DL for enhanced cybersecurity in IoT networks	CNNs, XAI	KDD CUP99, UNSW NB15, Bot-IoT	Accuracy, Interpretability
12	To propose a DL-based framework, IIDNet, for efficient cyberattack detection and classification in IoT environments	CNN, DR, Feature Engineering	UNSW-NB15	Precision, Recall, F1-Score, Accuracy
13	To propose EBIDS utilizing BERT for efficient ID in resourceconstrained IoT environments	BERT, Anomaly Detection	Edge-IIoT, CICDos 2017	Detection Accuracy, Computational Overhead, Realtime Performance
14	To propose a DL-based IDS for IoT networks that effectively detects cyber threats	LSTM, Dense Layers, Temporal & Spatial Dependencies	CICIDS2017	Accuracy, Loss Metrics, Robustness to Noise
15	To design a cybersecurity attack detection system for IIoT using an ensemble DL model	Ensemble DL, Honey-Badger Algorithm, LEOA	TON-IoT	Accuracy, Precision, Recall, F1score, MCC
16	To design and enhance an AIDS for IoT networks	SAE, CNN	Bot-IoT	Accuracy, Precision, Recall, F1Score, FPR, TPR
17	To develop a high-performance FPGA-based IDS for real-time communication security	MEL, XGBoost, HDL	NSL-KDD, IoTID20, CICIDS2017, UNSW NB15	Detection Rate, False Positive Rate, Real-time Operation
18	To enhance NID accuracy in IoT environments using DL and synthetic data generation	DL, CTGAN, Spatial and Temporal Feature	UNSW-NB15, CIC-IDS2018,	Classification Accuracy, MultiClass

		Extraction	CICIOT2023	ID, Data Imbalance Handling
19	To enhance ID accuracy in WSNs using SAPGAN optimized by NBOA	IDS-SAPGAN-NBOA-WSN	WSN-DS	Accuracy, Precision, Sensitivity
20	To analyze and address security challenges in IoT across diverse layers	Layered Analysis, Coss-Layer Integration	Benchmark Dataset	Security Issues, Solutions Comparison
21	To detect DDoS attacks efficiently in IoT environments using DL	HFPODL-DDoSCD, SA-BiTCNBiGRU, STO, APO	Standard Dataset	Accuracy, Precision, Recall, F-score, MCC
22	To discuss IoT security challenges, defences, and future research directions	Taxonomy of Security Challenges and Defense Mechanisms	NA	NA
23	Enhance 5G network security with a CCNN and EDO	CCNN, EDO	Benchmark Dataset	Accuracy, Robustness, Scalability
24	To enhance authentication and access control in IoT applications using semantic LSTM and BC	Semantic LSTM with BC	Standard Dataset	Computational Overhead, Scalability, Information Security
25	To enhance zero-day exploit detection with a probabilistic composite model for improved accuracy, time, and adaptability	AWPA-Autoencoder, MATA, GMCO, AHEDNet	UGRansome	Accuracy, Precision, Recall, F1-score, R^2 score, MCC, Cohen's Kappa, and Jaccard score
26	To develop a multi-attack IDS for MANETs with optimized node mobility and energy consumption	Centrality COA, MSA-GCNN	NS-2 Network Simulator	Accuracy, Precision, Recall, ROC
27	To improve IIoT anomaly detection accuracy and efficiency with a deep residual SConv1D-Attention model	SConv1D-Attention, bPSO	CICDDoS2019, NSL-KDD, X-IIoTID	ACC, DR, FPR, Precision, F1Score
28	To detect and classify ransomware threats using an EDVT model	EDVT, MSSAN, HTCEO	Benchmark Dataset	Accuracy, F1-Score, Recall, Detection Rate, MCC, Precision
29	To improve ID accuracy and speed in IoT networks using a 3D DL approach	3DLBS, CNN, LSTM, BCHO	ToN-IoT, UNSWNB15	Accuracy, Feature Reduction
30	To develop a BC-assisted cybersecurity solution for DDoS attack detection in IoT	EMDLM-BCCS, ELM, EGOA, BC	BoT-IoT	Detection Accuracy, Performance Improvement
31	To enhance cybersecurity in IIoT by utilizing advanced IDS models for detecting cyberthreats	MLP, CNN, RF, Hybrid DL	WUSTL-IIoT-2021	F1 Score, Accuracy, Recall, and Precision
32	For efficient anomaly detection and classification in IIoT using DL techniques	DLAD, ICSA, SRNN, HHO	NSL-KDD	Detection Accuracy, Feature Subset, Classification Performance
33	To develop an efficient IDS for IoT using optimized feature selection	EGWO for FS, RF Classification	NF-ToN-IoT	Accuracy, Feature Selection, Convergence
34	To develop a quantum-inspired BC-assisted cybersecurity model for IoT	FJCSA for Key Optimization, AALSTM-Ab for ID	Standard Dataset	Accuracy, Precision
35	To propose DFCCNN-BWOA-IDC for ID in cloud computing	DFCCNN with BWOA	DARPA	Accuracy

36	To develop an optimized ANN model for phishing email detection using BERT and COA	ANN with Soft Attention, BERT Encoders, and COA	Benchmark Dataset	Accuracy
37	To develop a multimodal biometric recognition system for secure authentication using palm and knuckle veins	Contrast-Enhancement, GLCM, DWT, ChOA, DNN	Benchmark Dataset	Accuracy, Sensitivity, Specificity
38	To develop a robust network security system for cyber threat detection using DL and metaheuristics	WSSA, SFLA, CAE	N-BaIoT	Accuracy, Precision, Recall, F-score, MCC

Table 1. Summary of AI-driven cybersecurity systems for IoT using DL and metaheuristic algorithms.

Data normalization: min–max normalization

At first, the data normalization stage employs min–max normalization to ensure consistency, accuracy, and efficiency by organizing data into a standardized format[39]. This model is chosen for this model because it effectually scales the data to a consistent range, usually between 0 and 1, which improves the convergence speed and performance of ML models. This method is specifically advantageous when dealing with datasets with varying magnitudes across features, as it ensures that no single feature dominates due to its scale. Unlike other

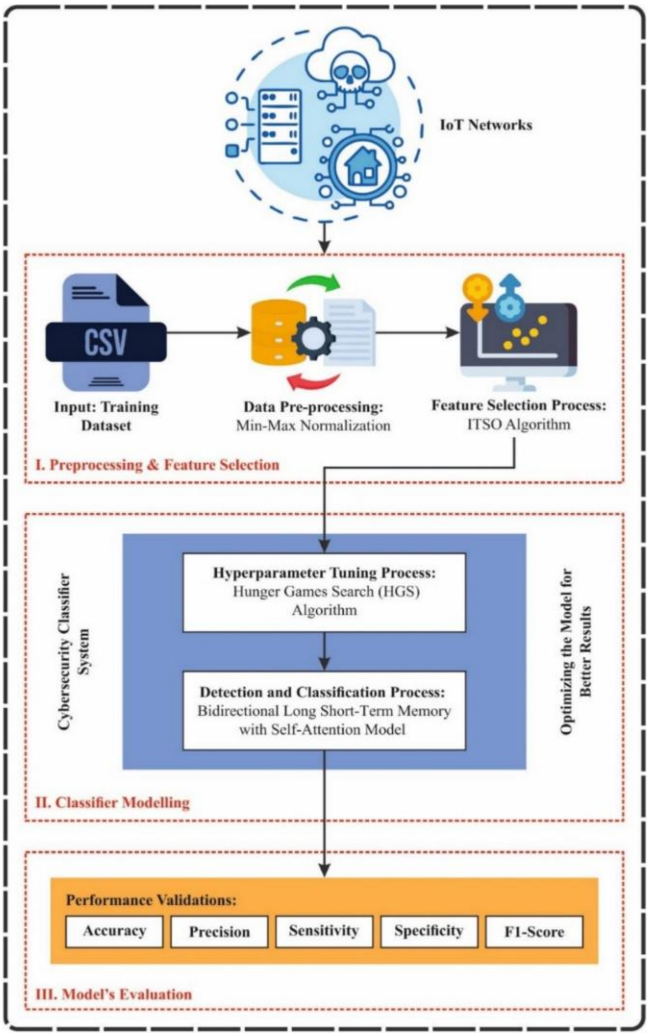

IoT Networks
CSV
Input: Training Dataset
Data Pre-processing: Min-Max Normalization
Feature Selection Process: ITSO Algorithm
I. Preprocessing & Feature Selection
Cybersecurity Classifier System
Hyperparameter Tuning Process: Hunger Games Search (HGS) Algorithm
Detection and Classification Process: Bidirectional Long Short-Term Memory with Self-Attention Model
Optimizing the Model for Better Results
II. Classifier Modelling
Performance Validations:
Accuracy
Precision
Sensitivity
Specificity
F1-Score
III. Model's Evaluation

Fig. 2: Overall process of ICSSADL-MHOA technique.

techniques, such as Z-score normalization, which assumes data is usually distributed, min–max normalization works well even for non-linear data distributions. It's also simple to implement and computationally efficient. Furthermore, this technique preserves the relationships between data points, making it appropriate for optimization-based models like the one in this framework. Maintaining consistency in feature scaling makes the model less prone to bias from outliers, resulting in more accurate results in classification and prediction tasks.

Normalization is significant in carrying out input data onto magnitude alterations of ML and DL techniques, which are complex to magnitude alterations. To attain that, Min-Max normalization is used to regularize the features in the interval of [0,1]. It is mathematically expressed below:

$$\mathrm{X} = \max B(X-)\min - \min(X)(X)$$

Here, B denotes a value of the original data; $min(X)$ and $Max(X)$ represent the minimum and maximum values, respectively; z means a significant normalization to prevent certain features from leading others owing to their measure.

DR: ITSO model

Next, the ITSO method is implemented for the feature selection process to detect the most relevant features in the data[40]. This model is chosen because it can effectively explore and exploit the search space, detecting the most pertinent features while avoiding redundant or irrelevant ones. Unlike conventional feature selection methods, ITSO replicates tuna's foraging behavior, allowing it to navigate complex, high-dimensional data spaces effectively. This swarm-based algorithm balances global exploration and local exploitation, making it specifically effective for massive datasets. The adaptive nature of the ITSO model ensures that it converges to optimal or near-optimal solutions without getting trapped in local minima, a common issue with other methods like greedy algorithms or filter-based techniques. Moreover, ITSO doesn't require prior knowledge of feature correlations, making it more versatile across diverse datasets. Its integration with ML techniques significantly improves accuracy by mitigating dimensionality and focusing on the most impactful features. Figure 3 illustrates the steps involved in the ITSO model.

The TSO model is a bio-inspired meta-heuristic model that originated from the tuna fish's foraging behavior. The foraging model consisted of dual phases in-depth, as demonstrated. The first model is spiral foraging, while tuna utilizes a spiral that forms throughout the search. This model permits them to flock their prey into less deep waters, making it easy to achieve. By accepting this spiral approach, tuna successfully enclose their prey and improve their probabilities of an effective search. The next model, parabolic foraging, includes all tunas following along, making a parabolic design to surround its prey successfully. By imitating these strategies, the TSO model improves its optimizer procedures. The mathematical model of these behaviors is described below:

Initialization

Like other bio-inspired meta-heuristic models, TSO initiates the optimization procedure by arbitrarily generating primary populations uniformly distributed through the searching region utilizing Eq. (2).

$$X_i^{int} = rand.(ub - lb) + lb, i = 1_t 2_t NP$$

whereas $x^{int}{}_i$ denotes i^{th} individual; ub and lb represent the upper and lower limits, respectively; NP characterizes the tuna population counts, and the $rand$ refers to uniformly distributed arbitrary vectors with values ranging between (0−1).

Spiral foraging

When encountered with predators, smaller breeding fishlike herring and sardines exhibit dynamic behavior, constantly adjusting their swimming direction to evade threats. In contrast, tuna schools use a tightly looped spiral formation to pursue their prey. While most fish may lack robust orientation skills, they collaborate with more adept swimmers, forming a cohesive, unified hunting force. Furthermore, tuna schools share information with all members following the lead fish, enabling effective communication and coordinated movements.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 8, Issue 3, May-June 2025||

DOI:10.15662/IJRAI.2025.0803010

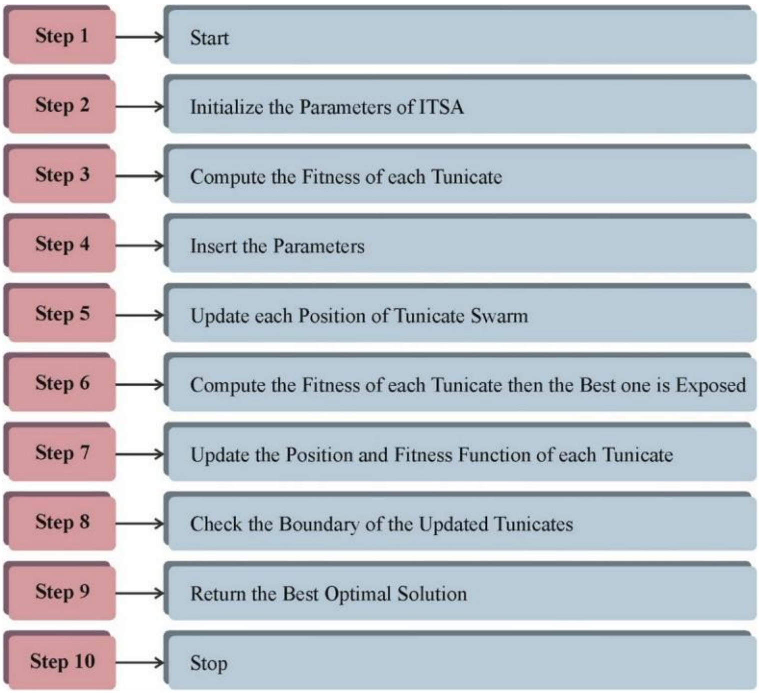

Step 1
Start
Step 2
Initialize the Parameters of ITSA
Step 3
Compute the Fitness of each Tunicate
Step 4
Insert the Parameters
Step 5
Update each Position of Tunicate Swarm
Step 6
Compute the Fitness of each Tunicate then the Best one is Exposed
Step 7
Update the Position and Fitness Function of each Tunicate
Step 8
Check the Boundary of the Updated Tunicates
Step 9
Return the Best Optimal Solution
Step 10
Stop

Fig. 3: Steps involved in the ITSO method.

The foraging behavior also comprises a concept where if a group member fails to find food, the rest do not blindly follow. Instead, a random reference point within the search space is introduced to guide the spiral search.

This encourages broader exploration and improves the group's global search capability.

The updated model for the group members' movement is as follows:

$$X \quad = \quad a1.\ X \quad + \beta.\ X \quad + a2.X\ ,i = 1$$
$$t{+}1\ a1.Xbestt\ \ +besttβ.Xbestt\ \ −besttXit\ +ita2.Xit−1,iit= 2,3,..NP$$

This model facilitates global exploration, enhancing the overall search efficiency by diversifying the strategy of the group

$$1 = a^{\ +\,(1} - a).$$
$$\alpha 2 = (1 - a) - (1 - a)._{t}\mathrm{max}$$
$$\beta = e^{bl}.cos(2\pi b)\quad l = e3.cos(((\mathrm{tmax} + \tau\underline{1}) - 1)\pi)$$

The equations describe an optimization process where the position of everyone, X_i^{t+1}, is updated based on the best-known solution, $X_{best}{}^{t}$, and the previous position of an individual. The constants $\alpha 1$ and $\alpha 2$ control the extent to which individuals depend on the optimal solution and their prior positions during the search. The parameter β, computed utilizing a random factor b, introduces the agent's movement variability. , defined as a dynamic spiral factor, improves global exploration. The variables t and $t_{\max}$ represent the current and maximum iteration counts. The random number b is uniformly distributed between 0 and 1, guiding the exploration– exploitation balance in the optimization process. These dynamics ensure that the group maintains an efficient and diverse search strategy.

Parabolic foraging

In addition to the spiral feeding form, tunas participate in cooperative feeding by accepting a parabolic pattern. In this design, they utilize reference points that are usually the position of their food. In addition, tunas dynamically look for food in their direct environments. These double-feeding models are implemented together, with an equivalent presumed probability of 50%. The mathematic representation which designates this phenomenon is defined as shown:

Classification process: BiLSTM-SA

Besides, the proposed ICSSADL-MHOA model utilizes the BiLSTM-SA technique for the classification method of cybersecurity[41]. This model is chosen because it can capture both past and future dependencies in sequential data. The bidirectional nature of BiLSTM allows the model to access context from both directions, enhancing its capability to comprehend temporal relationships and patterns that may exist in the data. When integrated with SA, the model can concentrate on the most relevant parts of the input sequence, allowing it to emphasize crucial features while disregarding irrelevant ones. This makes it highly effective for complex, dynamic datasets like those encountered in cybersecurity. Unlike conventional models that may face difficulty with long-range dependencies, BiLSTM-SA outperforms learning from sequences of varying lengths. Furthermore, integrating LSTM and attention mechanisms improves its robustness, enabling it to perform better in detection and classification tasks than simpler models like conventional feedforward neural networks or shallow LSTMs. Figure 4 depicts the infrastructure of BiLSTM-SA.

The networks of the LSTM technique control the information flow over gating mechanisms, allowing them to read, retain, and remove information. These networks are effectual in taking long-term dependences and, partially, easing the tasks of gradient explosion and vanishing that recurrent neural networks (RNNs) might face when handling long successive data. It has numerous memory cells, and each one has anf_t forget gate, i_t s input gate, and 0_t output gate:

$$f_t = \sigma \left(W_f \cdot [h_{t-}1, x_t] + b_f\right)$$

$$i_t = \sigma \left(W_i \cdot [h_{t-}1, x_t] + b_i\right)$$

$$o_t = \sigma \left(W_o \cdot [h_{t-}1, x_t] + b_o\right)$$

In Eq. (12), σ is an sigmoid activation function; W and b signify the weight matrix and bias, respectively; $h_{t-}1$ represents the preceding moment's hidden layer (HL); x_t is a present input.

The input gate defines what present input data must be kept in the memory cell. The forget gate mainly defines how many preceding memories must be left out. The memory cell concludes which data wants to be removed and must be remembered for the following step per the verdicts created by both input and forget

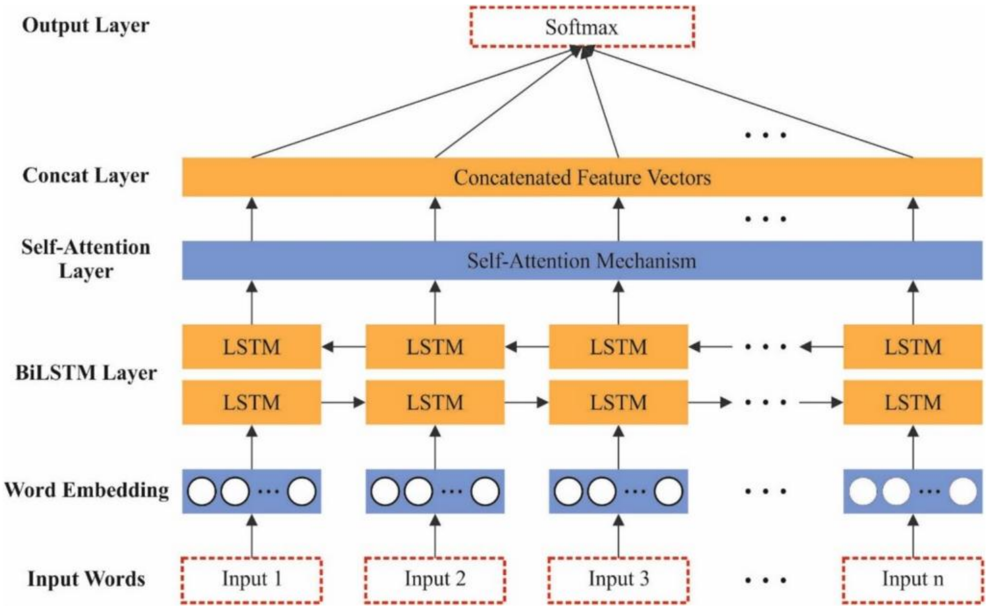


Fig. 4: Structure of BiLSTM-SA approach.

gates. The gate of output manages a quantity of data, which is distributed from the memory cell to HL. Then, it is employed as an output and distributed to the following layer. The final output value has been computed by enlarging the output gate and outcomes by the memory cell. On the other hand, LSTM can only deal with data in a one-way method, generally from the start to the end of the series. To overwhelm this restraint, the BiLSTM technique employs dual dissimilar layers of LSTM at every time step: one handles the sequence in the direction forward (from start to finish), and other handles it backwards (from finish to start).

The main aim of BiLSTM is to take bidirectional dependencies by uniting outputs from both directions. This bidirectional model permits the method to incorporate context data by seizing intricate dependencies in sequences.

SA is commonly employed in CV and NLP methodologies to capture links within sequences. The main goal is to permit the method for handling inputs at every step by reflecting local district data and focusing on other fragments of similar input series. This flexibility allows the process to seize global dependencies among basics by spreading. Furthermore, SA provides the benefit of sequential handling instead of handling simultaneously. This method can alter the attention weights across numerous time-steps by providing more concentration to significant steps.

Initially, inputs are changed into 3 vectors such as key (K), query (Q), and value (V). Then, the resemblance was computed utilizing the dot product among Q and K, followed by standardization of the similarity scores for getting attention weight. Then, they are employed in the value vectors, and the resultant output is weighted completely:

$$Q = XW_q,K = XW_k,V = XW_v$$

Here, W_q,W_k, and W_v denote the weight matrices. The dot product of K and Q was employed for calculating their resemblance:

$Attention\ (Q,K,V\ ) = softmax(^{QK}\sqrt{}\_\_^{T})V$ (16) $_dk$

In the equation mentioned above, d_k denotes the key dimension employed for measuring the dot product to evade the problem of gradient explosions or vanishing. S *oftmax* regularizes the resemblance scores for getting attention weights and next attains a weighted synopsis on vector V to attain the last output:

$$Output = Attention\ (Q,K,V\ )$$

Parameter optimizer: HGS model

Finally, the parameter selection of the BiLSTM-SA is executed using the HGS method[42]. This method is chosen because it can optimize complex, high-dimensional search spaces. Unlike conventional optimization techniques, such as grid or random search, HGS is inspired by natural selection processes, which enables it to balance exploration and exploitation more effectively. This method adapts to dynamic environments, making it ideal for optimizing the parameters of DL methods such as BiLSTM-SA. HGS can avert local minima, a common challenge in parameter tuning, by integrating diverse strategies that improve global exploration.

Additionally, HGS can handle large search spaces with a reduced computational cost compared to exhaustive search methods. Its robustness and capability to fine-tune hyperparameters make it specifically appropriate for enhancing the performance of complex models like BiLSTM-SA, ultimately improving the classification accuracy and efficiency of the cybersecurity system. Figure 5 specifies the steps involved in the HGS technique.

The HGS is the recent and novel population-based meta-heuristic method, which imitates the natural insight of animals to look for food. Hunger has been the primary inspiration for designing a competitive and computationally efficient model. The model mimics selection, competition, and adaptive procedures existing naturally, along with imaginary games (Hunger Games). In such games, individuals (agents) challenge survival or resources in challenging surroundings. During the optimization context, these individuals are considered promising solutions to problems, and the surroundings are the region, while the difficulties are to be investigated for solutions. The model passes across the selection, adaptation, and competition methods, which assist in making the optimal solution(s) to the problem. This segment describes the mathematical representation of the HGS method. The model depends on dual key elements, the *HungerRule* and the *ApproachRule*, to mimic adaptive decision-making strategies and natural hunger-driven behaviors.

Approaching food

Naturally, animals often cooperate in looking for food, whereas in other cases, they select to hunt autonomously. Animal searching models stimulate the mathematic equation in Eq. (18). They characterize three dissimilar models in which animals transfer, imitating their behaviour once they approach a food source. These designs are essential to the HGS approach, which imitates individual foraging or cooperative behaviour between animals.

$-\!\!\rightarrow_X ({}_t + 1) =$ □□□□ $-W\rightarrow \cdot \rightarrow -X \cdot bb(1 ++ \rightarrow -Rrandn \cdot -W\rightarrow 22 \cdot (1))\rightarrow -Xbb, - \rightarrow -X(t), ifrifr111 >< ll,r22 > E$ (18) $-\!\!\rightarrow X(t)$

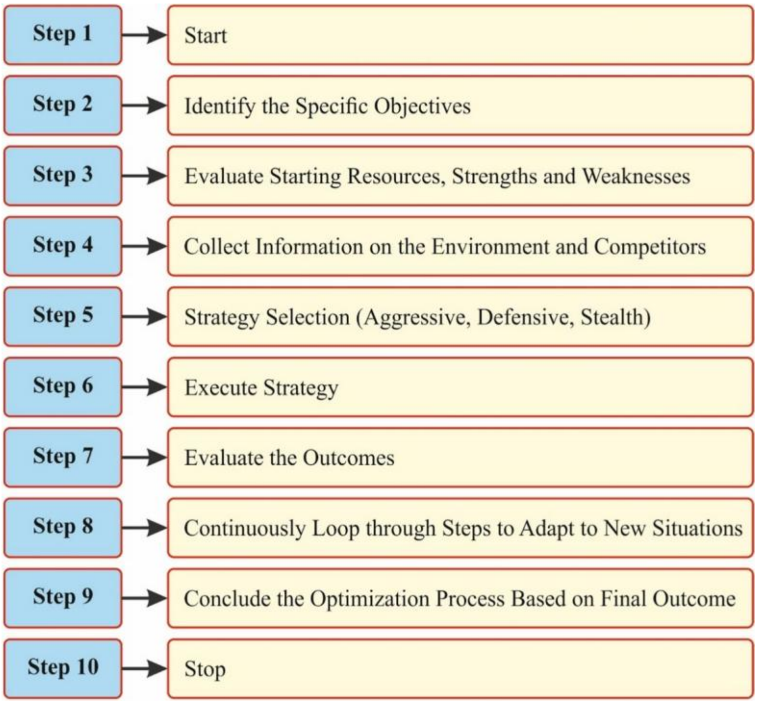

Step 1
Start
Step 2
Identify the Specific Objectives
Step 3
Evaluate Starting Resources, Strengths and Weaknesses
Step 4
Collect Information on the Environment and Competitors
Step 5
Strategy Selection (Aggressive, Defensive, Stealth)
Step 6
Execute Strategy
Step 7
Evaluate the Outcomes
Step 8
Continuously Loop through Steps to Adapt to New Situations
Step 9
Conclude the Optimization Process Based on Final Outcome
Step 10
Stop

Fig. 5: Steps involved in the HGS methodology.

hunting ends after the individual is most starving, using R helping as a controller to decrease the range of activity to 0 slowly. The subtraction or addition of the range of activity, subjective by $-W\rightarrow 1 \cdot -\!\!\rightarrow Xb$, imitates how an individual, directed among their peers to food resources, restarts hunting at the present position after food is located. Now, $-W\rightarrow_1$ characterizes the difference in precisely locating the real position.

Based on the mathematical expression in Eq. (19), E assists as variation controls for each position.

$$E = \text{sech}(|F(i) - BF|)$$

For all individuals i, whereas i range between (1-n) using n to become the quantity of population size or searching agents, $F(i)$ signifies the fitness value. BF indicates the optimal fitness attained in the present iteration (thus far). The function of hyperbolic *sech* was described as follows: ^{2}

$sech(x) =$ _______

$ex + e_{-}x$

The expression for $-\!\!\rightarrow R$ is delineated as:

$$-\!\!\rightarrow R = 2 \times shrink \times rand - shrink$$

$$shrink = 2^{\times} (1 - \_^{t})$$

Now, *rand* characterizes a randomly generated value inside the range [0,1], and *T* signifies the total iteration counts. The shrinking parameter, computed according to the present iteration *t* according to the total iterations *T*, ranges between (0−2). These ranges consider how the impact on the *shrink* factor reduces in time, from its maximum at the beginning of the searching procedure to 0 as *t* approaches *T*. Therefore, the *R* range that fine-tunes the activities range the search agents derived from *rand* and *shrink*, further differs from 2 to 2. This dynamical range permits a measured exploration of searching region, restricting as the model grows, to concentrate on exploiting optimal solutions discovered.

Hunger rule

This part presents the mathematical method miming individuals' starvation qualities, establishing the HGS method's core concept.

$-W\rightarrow 1\ (i) = \quad hungry\ (i) \cdot \quad \cdot r4, \quad \overline{\quad\quad} ifr3 < l$

$\{ 1, \quad SHhungryN \quad ifr3 > l$

$-W\rightarrow 2\ (i) = (1 - \exp(-|hungry\ (i) - SH_{hungry}|)) \cdot r5 \cdot 2$

Given that hunger calculates every individual's hunger level, *N* represents the entire individual count, and

Σ *SHungry* characterizes the aggregated hunger through every individual, calculating their hunger levels (*hungry*). r_3, r_4, and r_5 random numbers fall under the range [0,1]. The equation for computing a hungry individual, *hungry*(*i*), is delineated in Eq. (25).

$_{hungry}\ (_i) = \{\ hungry0(,ifAllFitnessi) + H,ifAllFitness(i) = BF(i)\ ^{=}\!/$

Here, *AllFitness*(*i*) collects the fitness values of all individuals for the present iteration. At all iterations, the best-performing individual's hunger level returns to 0. The upgraded hunger levels are denoted by *H*. The *H* value is computed utilizing Eq. (26).

$H = \{\ LH \cdot_{TH,ifTH}(1 + r),ifTH < LH \geq_{LH}$

$$= \frac{F(i) - BF}{WF - BF} \cdot r_6 \cdot 2 \cdot (UB - LB)$$

whereas r_6 represents a randomly generated amount within the interval of [0,1]; *F*(*i*) signifies the fitness value of all individuals; *BF* characterizes the maximum fitness attained in the present iteration; *WF* indicates the low fitness gained in the present iteration; *LB* and *UB* stands for the lower and upper limits of the feature area, respectively. As defined, the hunger sensation signifies minimal values, *and limits*. To improve the model's efficacy, hunger's lower and upper thresholds are processed by using the value of *LHs* to be explored in parameter tuning. Hunger can impact the range of activity either negatively or positively. W_1 and W_2 are demonstrated to reflect that. During Eq. (28), the disparities amongst *LB* and *UB* demonstrate the maximal hunger level in changing states; hunting possible in the present situation; *F*(*i*) − *BFFWFi* determines the remaining food needed for the individual to fulfil *DFDF WF* − *DF* computes an individual's total 2 evaluates the environmental starvation; Eve~~ry iteratio~~n changes the hunger level of an individual.
( )− controls the hunger ratio; *r*6 x

− influence, both positive and negative, on hunger.

The HGS approach originates an FF for getting an enhanced classification of performance. It explains a positive number to imply the better result of the candidate solution. At this point, the classification error rate reduction is measured as FF. Its formulation is expressed below:

$fitness(x_i) = classifierErrorRate(x_i)$

$= no.\ of\ misclassified\ samples\ Totalno.\ of\ samples \times 100$

IV. EXPERIMENTAL VALIDATION AND DISCUSSION

The simulation analysis of the ICSSADL-MHOA technique is examined under dual datasets such as ToNIoT[43]and Edge-IIoT[44]. The ToN-IoT database contains 119,957 no. of samples below nine class labels. The total number of features is 42, but only 27 have been selected. The complete details of this dataset are depicted in Table 2. The suggested technique is simulated using the Python 3.6.5 tool on PC i5-8600 k, 250 GB SSD, GeForce 1050 Ti 4 GB, 16 GB RAM, and 1 TB HDD. The parameter settings are provided: learning rate: 0.01, activation: ReLU, epoch count: 50, dropout: 0.5, and batch size: 5.

Figure 6 displays the classifier results of the ICSSADL-MHOA model on the ToN-IoT dataset. Figures 6a6b displays the confusion matrices by accurately identifying and classifying all classes below 70%TRPH and 30%TSPH. Figure 6c presents the PR study, which notified higher performance through all classes. At last, Fig. 6d demonstrates the ROC study, which illustrates skilful solutions with significant values of ROC for different class labels.

The results from Table 3 and Fig. 7 show the performance of the ICSSADL-MHOA approach for detecting cyberattacks on the ToN-IoT dataset under two diverse attack proportions: 70% TRPH and 30% TSPH. For 70% TRPH, the method illustrates high accuracy, with an average $accu_y$ of 99.42%, indicating superior performance in identifying standard and attack class labels. The $prec_n$ of 92.51% suggests an effectual reduction of false positives, while the $sens_y$ of 87.79% shows the capability of the model to detect a high percentage of true positive attack instances. However, this sensitivity represents that some minority class attacks, like MiTM, may also not be detected, suggesting room for improvement. The $spec_y$ of 99.53% demonstrates the capability of the technique to accurately detect normal instances without false positives, and the $F1_{score}$ of 89.13% reflects a balanced $prec_n$ and recall. For 30% TSPH, the performance slightly decreases, with an $accu_y$ of 99.44%, $prec_n$ of 92.17%, $sens_y$ of 87.76%, $spec_y$ of 99.56%, and an $F1_{score}$ e of 88.99%. The slight reduction in $sens_y$ for both configurations points to challenges in detecting rare attacks, specifically under imbalanced data conditions. This reduction could be addressed by techniques like resampling or weighted loss functions to enhance the detection of low-frequency attacks.

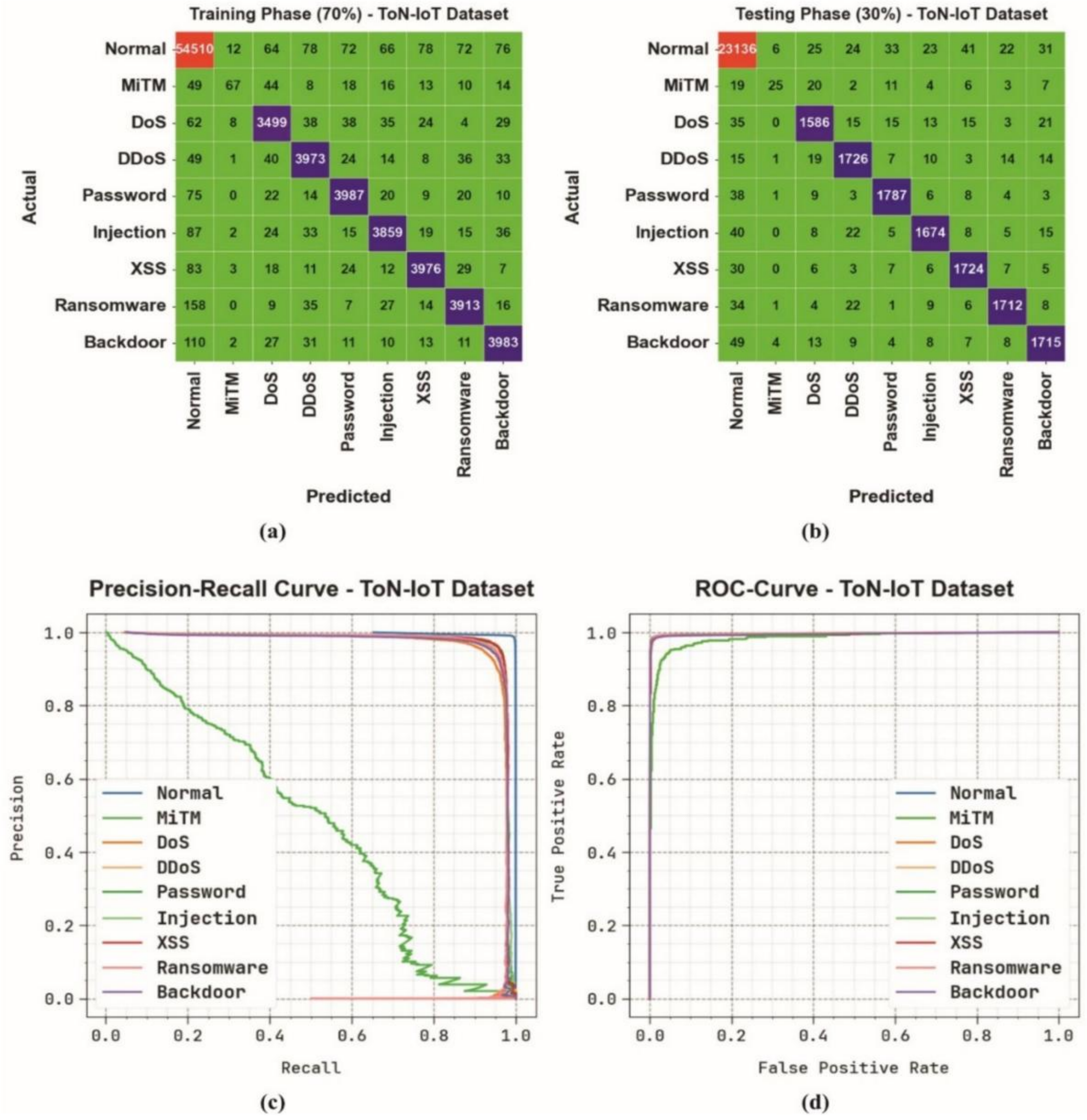
In Fig. 8, the training (TRA) and validation (VAL) $accu_y$ performances of the ICSSADL-MHOA technique on the ToN-IoT dataset are exemplified. The values of $accu_y$ are computed across a period of 0–25 epochs. The figure underscored that the values of TRA and VAL $accu_y$ present a cumulative tendency indicating the proficiency of the ICSSADL-MHOA method through maximum performance through multiple repetitions. In addition, the TRA and VAL $accu_y$ values remain close through the epochs, notifying lesser overfitting and revealing the maximum outcome of the ICSSADL-MHOA method, which guarantees steady prediction on unseen samples.

Figure 9 shows the TRA loss (TRALOS) and VAL loss (VALLOS) of the ICSSADL-MHOA approach on the ToN-IoT database. The loss values are computed throughout 0–25 epochs. The values of TRALOS and VALLOS depict a diminishing trend, which indicates the proficiency of the ICSSADL-MHOA approach in harmonizing a tradeoff between generalization and data fitting. The consecutive decrease in loss and securities values improved the performance of the ICSSADL-MHOA technique and tuned the prediction results after a while.

Table 4 and Figs. 10–11 shows the comparative study of the ICSSADL-MHOA approach on the ToNIoT dataset with existing methodologies below different metrics. The performances imply that the proposed ICSSADL-MHOA approach has improved outcome $accu_y$ of 99.44%, $prec_n$ of 92.17%, $sens_y$ of 87.76%, $spec_y$

ToN-IoT Database	
Classes	**No. of Instances**
“Normal”	78,369
“MiTM”	336
“DoS”	5440
“DDoS"	5987
“Password”	6016
“Injection”	5867
“XSS”	5951
“Ransomware”	5976
“Backdoor”	6015
Total Instances	**119,957**

Table 2. Details of the dataset.



(a) (b)

(c) (d)

Fig. 6: ToN-IoT dataset **(a-b)** Confusion matrices and **(c-d)** curves of PR and ROC.

of 99.56%. While the existing models DT, RF, KNN, SVM, XGBoost, MLP, and NB techniques have gained the poorest performance.

Also, the proposed ICSSADL-MHOA method is examined under the Edge-IIoT dataset. This dataset has 56,000 records under 12 classes, as represented in Table 5. The total number of features is 62, but only 45 have been selected.
Figure 12 displays the classifier results of the ICSSADL-MHOA model on the Edge-IIoT dataset. Figures 12a-12b depicts the confusion matrices through precise identification and classification of all classes below 70%TRPH and 30%TSPH. Figure 12c shows the PR examination, which notified superior performance over all class labels. Finally, Fig. 12d exemplifies the ROC examination, which demonstrates capable solutions with significant values of ROC for dissimilar class labels.

Table 6 and Fig. 13 demonstrate cyberattack detection of the ICSSADL-MHOA approach on the Edge-IIoT dataset below 70%TRPH and 30%TSPH is showcased. The performances show that the ICSSADL-MHOA model

Class Labels	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	$^{F}1score$
TRPH (70%)					
Normal	98.58	98.78	99.06	97.67	98.92
MiTM	99.76	70.53	28.03	99.97	40.12
DoS	99.42	93.38	93.63	99.69	93.51
DDoS	99.46	94.12	95.09	99.69	94.61
Password	99.55	95.02	95.91	99.74	95.46
Injection	99.49	95.07	94.35	99.75	94.71
XSS	99.57	95.71	95.51	99.78	95.61
Ransomware	99.45	95.21	93.63	99.75	94.41
Backdoor	99.48	94.74	94.88	99.72	94.81
Average	**99.42**	**92.51**	**87.79**	**99.53**	**89.13**
TSPH (30%)					
Normal	98.71	98.89	99.12	97.94	99.01
MiTM	99.76	65.79	25.77	99.96	37.04
DoS	99.39	93.85	93.13	99.70	93.49
DDoS	99.49	94.52	95.41	99.71	94.97
Password	99.57	95.56	96.13	99.76	95.84
Injection	99.49	95.49	94.20	99.77	94.84
XSS	99.56	94.83	96.42	99.73	95.62
Ransomware	99.58	96.29	95.27	99.81	95.78
Backdoor	99.43	94.28	94.39	99.70	94.33
Average	**99.44**	**92.17**	**87.76**	**99.56**	**88.99**

Table 3. Cyberattack detection of ICSSADL-MHOA method on ToN-IoT dataset.

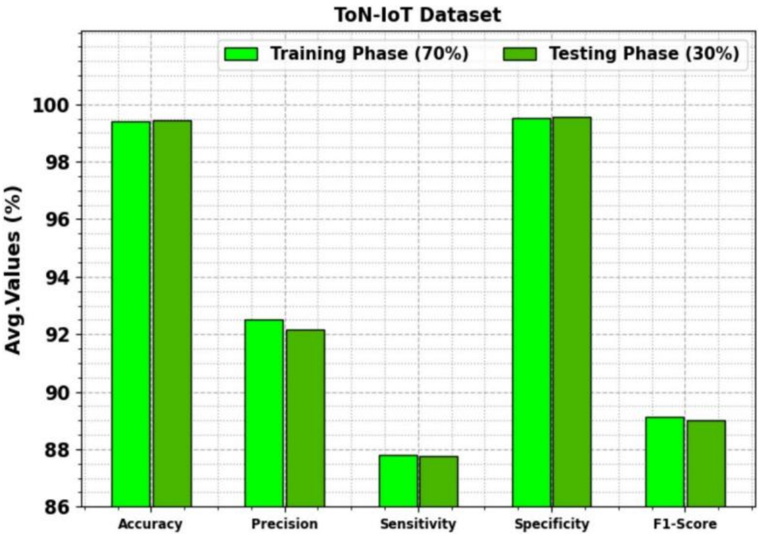


Fig. 7: Average of ICSSADL-MHOA model on ToN-IoT dataset.

.

efficiently detected all class labels. Based on 70%TRPH, the ICSSADL-MHOA approach attains an average $accu_y$ of 99.33%, $prec_n$ of 95.99%, $sens_y$ of 95.79%, $spec_y$ of 99.63%, and $F1_{score}$ of 95.88%. Moreover, according to 30%TSPH, the ICSSADL-MHOA approach attains an average $accu_y$ of 99.37%, $prec_n$ of 96.12%, $sens_y$ of 96.02%, $spec_y$ of 99.65%, and $F1_{score}$ of 96.07%.

Figure 14 depicts the TRA and VAL $accu_y$ performances of the ICSSADL-MHOA technique on the EdgeIIoT dataset. The values of $accu_y$ are computed through a period of 0–25 epochs. The figure underscored that the values of TRA and VAL $accu_y$ show an increasing trend, indicating the capacity of the ICSSADL-MHOA approach with maximum performance across numerous repetitions. Followed by the TRA and VAL $accu_y$ values remaining close across the epochs, notifying diminished overfitting and showing the maximal performance of the ICSSADL-MHOA approach, which assurances reliable prediction on unseen samples.

Figure 15 shows the TRALOS and VALLOS graph of the ICSSADL-MHOA methodology on the Edge-IIoT dataset. The loss values are computed throughout 0–25 epochs. The values of TRALOS and VALLOS represent

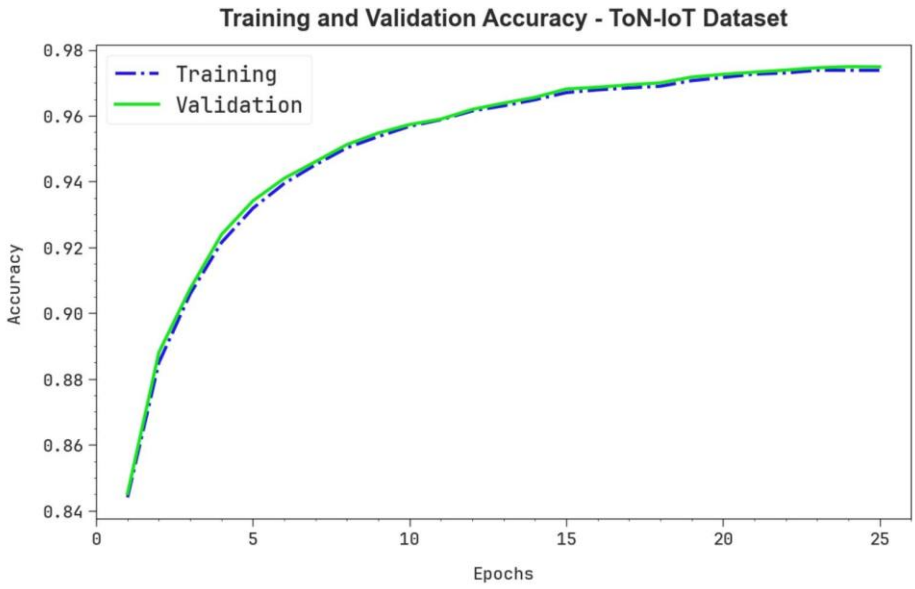


Fig. 8: *$Accu_y$* curve of ICSSADL-MHOA model on the ToN-IoT dataset.

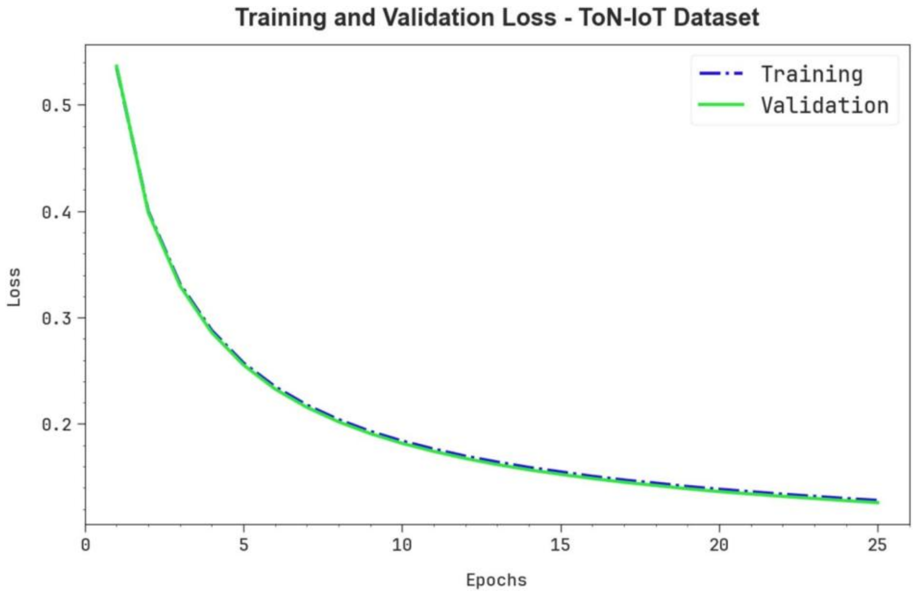


Fig. 9: Loss curve of ICSSADL-MHOA method on ToN-IoT dataset.

a declining trend, which indicates the proficiency of the ICSSADL-MHOA approach in harmonizing a tradeoff between data fitting and generalization. The successive dilution in values of loss and securities enhances and securities enhances the outcome of the ICSSADL-MHOA approach and tunes the calculation results gradually.

Table 7 and Figs. 16–17shows the comparative study of the ICSSADL-MHOA approach on the Edge-IIoT dataset with existing methodologies below different metrics[45–48]. The performances denote that the proposed ICSSADL-MHOA technique has gained superior outcome $accu_y$ of 99.37%, $prec_n$ of 96.12%, $sens_y$ of 96.02%, $spec_y$ of 99.65%. The existing methods, Shallow ANN, Isolated LSTM, CNN, RF, SVM, DNN, and Inception Time techniques, have achieved the poorest performance.

ToN-IoT Dataset				
Model	***$Accu_y$***	***$Prec_n$***	***$Sens_y$***	***$Spec_y$***
Decision Tree	87.50	79.52	79.10	95.67
Random Forest	87.50	89.15	79.15	97.85
kNN Algorithm	97.60	79.54	81.50	95.88
SVM Classifier	74.70	91.49	85.95	90.17
XGBoost	97.80	82.41	79.66	96.88
MLP Method	98.67	82.07	81.15	96.65
Naïve Bayes	99.22	84.81	84.41	98.11
ICSSADL-MHOA	99.44	92.17	87.76	99.56

Table 4. Comparative analysis of ICSSADL-MHOA method on the ToN-IoT dataset.

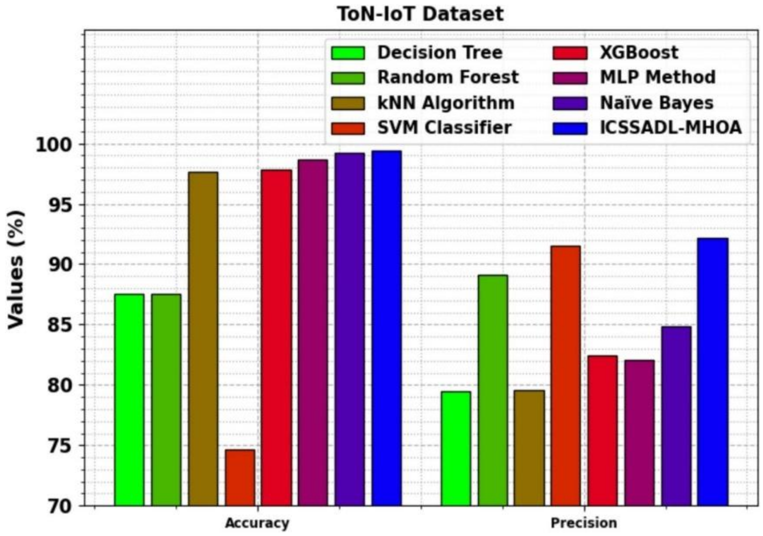


Fig. 10: Accu $_y$ and Prec $_n$ outcome of ICSSADL-MHOA technique on ToN-IoT dataset.

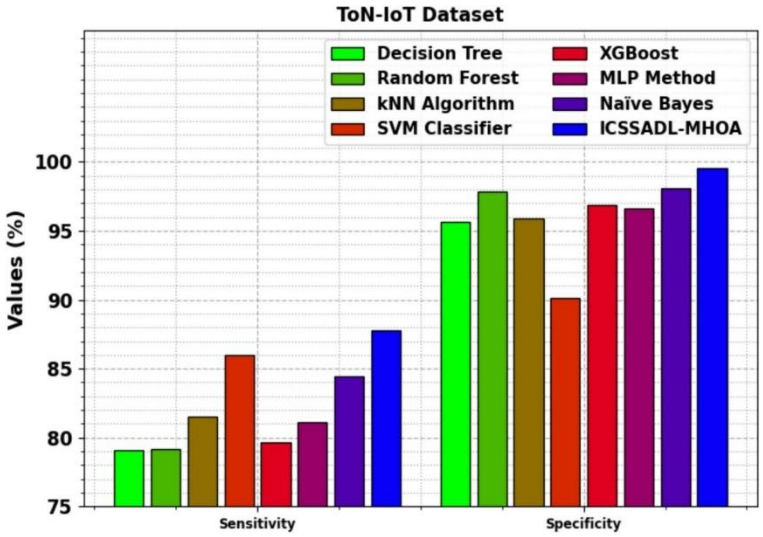


Fig. 11: Sens $_y$ and Spec $_y$ outcome of ICSSADL-MHOA technique on ToN-IoT dataset.

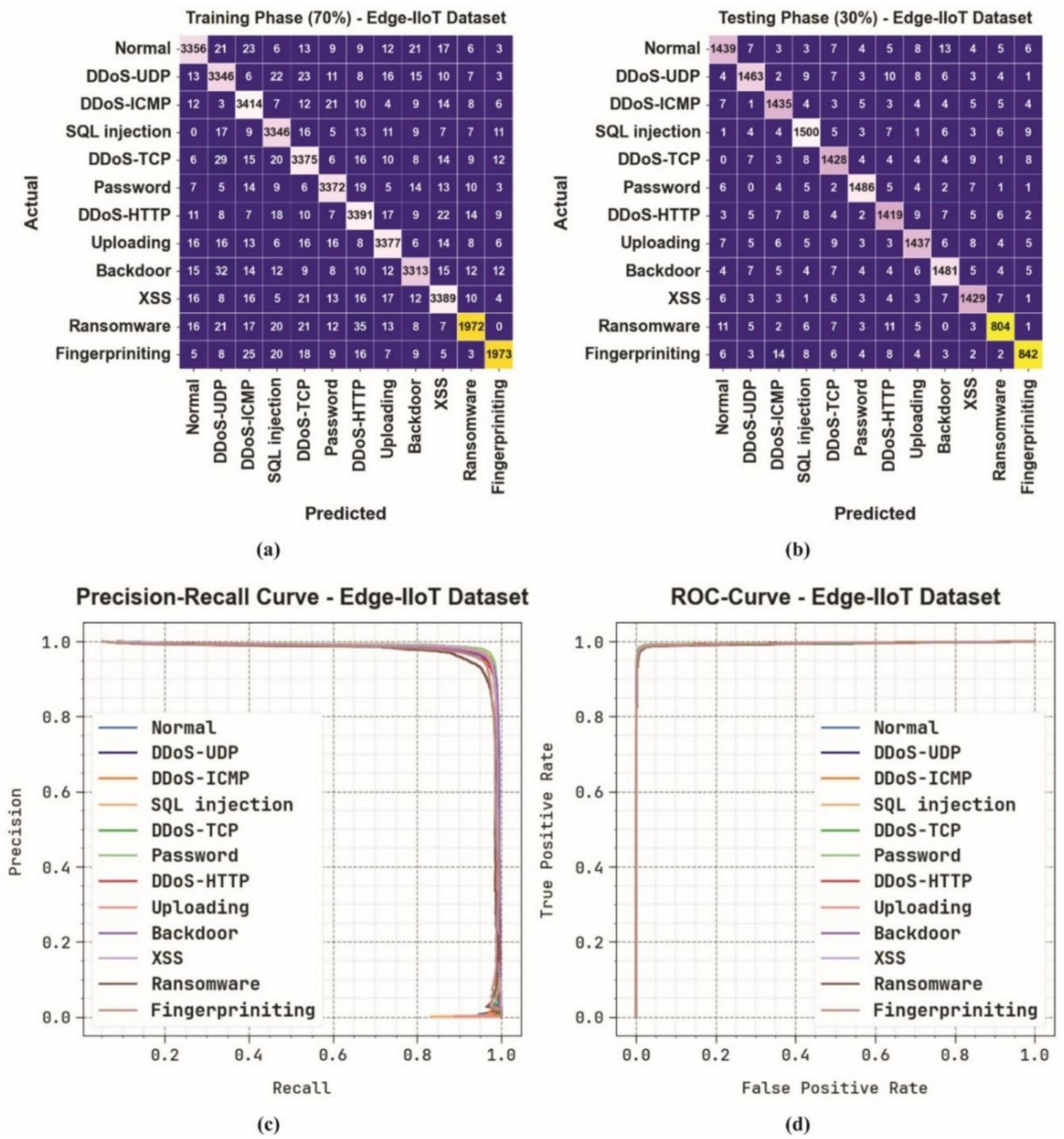
Edge-IIoT Dataset	
Types of Event	**Data Record**
Normal	5000
DDoS-UDP	5000
DDoS-ICMP	5000
SQL injection	5000
DDoS-TCP	5000
Password	5000
DDoS-HTTP	5000
Uploading	5000
Backdoor	5000
XSS	5000
Ransomware	3000
Fingerpriniting	3000
Total Record	**56,000**

Table 5. Details of Edge-IIoT dataset.

V. CONCLUSION

In this article, a new ICSSADL-MHOA technique is presented. The main aim of the ICSSADL-MHOA technique is to enhance a robust cybersecurity system in IoT networks. At first, the data normalization stage employs min– max normalization to ensure consistency, accuracy, and efficiency by organizing data into a standardized format. Next, the ITSO model was implemented for the FS process to detect the most relevant features in the data. Besides, the proposed ICSSADL-MHOA model designs the BiLSTM-SA technique for the classification method of cybersecurity. Finally, the parameter selection of the BiLSTM-SA is implemented using the HGS method. Comprehensive studies under the ToN-IoT and Edge-IIoT datasets validate the efficiency of the ICSSADLMHOA method. The experimental validation of the ICSSADL-MHOA method illustrated a superior accuracy value of 99.37% over existing techniques.

The ICSSADL-MHOA method's limitations include reliance on a limited set of data sources, which may not fully represent the diverse behavior of IoT environments and threats. Additionally, the computational complexity of specific approaches could affect their applicability in resource constrained devices, affecting scalability and real-time performance. The proposed models may also struggle to handle data imbalances and noisy environments, impacting the detection accuracy for minority class threats. Furthermore, many existing solutions fail to address cross-layer security challenges comprehensively, which is significant for robust IoT defense. Future work should improve the model's adaptability across diverse IoT systems, optimize computational efficiency, and develop hybrid techniques incorporating diverse security layers. Enhancing real-time detection capabilities and exploring lightweight solutions for edge devices would also be vital for the practical deployment of these methods. Additionally, further research could focus on integrating adversarial ML techniques to improve the system's robustness against sophisticated cyberattacks.



Training Phase (70%) - Edge-IIoT Dataset

	Normal	DDoS-UDP	DDoS-ICMP	SQL injection	DDoS-TCP	Password	DDoS-HTTP	Uploading	Backdoor	XSS	Ransomware	Fingerpriniting
Normal	3356	21	23	6	13	9	9	12	21	17	6	3
DDoS-UDP	13	3346	6	22	23	11	8	16	15	10	7	3
DDoS-ICMP	12	3	3414	7	12	21	10	4	9	14	8	6
SQL injection	0	17	9	3346	16	5	13	11	9	7	7	11
DDoS-TCP	6	29	15	20	3375	6	16	10	8	14	9	12
Password	7	5	14	9	6	3372	19	5	14	13	10	3
DDoS-HTTP	11	8	7	18	10	7	3391	17	9	22	14	9
Uploading	16	16	13	6	16	16	8	3377	6	14	8	6
Backdoor	15	32	14	12	9	8	10	12	3313	15	12	12
XSS	16	8	16	5	21	13	16	17	12	3389	10	4
Ransomware	16	21	17	20	21	12	35	13	8	7	1972	0
Fingerpriniting	5	8	25	20	18	9	16	7	9	5	3	1973

(a)

Testing Phase (30%) - Edge-IIoT Dataset

	Normal	DDoS-UDP	DDoS-ICMP	SQL injection	DDoS-TCP	Password	DDoS-HTTP	Uploading	Backdoor	XSS	Ransomware	Fingerpriniting
Normal	1439	7	3	3	7	4	5	8	13	4	5	6
DDoS-UDP	4	1463	2	9	7	3	10	8	6	3	4	1
DDoS-ICMP	7	1	1435	4	3	5	3	4	4	5	5	4
SQL injection	1	4	4	1500	5	3	7	1	6	3	6	9
DDoS-TCP	0	7	3	8	1428	4	4	4	4	9	1	8
Password	6	0	4	5	2	1486	5	4	2	7	1	1
DDoS-HTTP	3	5	7	8	4	2	1419	9	7	5	6	2
Uploading	7	5	6	5	9	3	3	1437	6	8	4	5
Backdoor	4	7	5	4	7	4	4	6	1481	5	4	5
XSS	6	3	3	1	6	3	4	3	7	1429	7	1
Ransomware	11	5	2	6	7	3	11	5	0	3	804	1
Fingerpriniting	6	3	14	8	6	4	8	4	3	2	2	842

(b)

Precision-Recall Curve - Edge-IIoT Dataset

(c)

ROC-Curve - Edge-IIoT Dataset

(d)

Fig. 12: Edge-IIoT dataset (a-b) confusion matrices and (c-d) curves of PR and ROC.

Class Labels	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	^F1score
TRPH (70%)					
Normal	99.34	96.63	96.00	99.67	96.31
DDoS-UDP	99.23	95.22	96.15	99.53	95.68
DDoS-ICMP	99.32	95.55	96.99	99.55	96.26
SQL injection	99.36	95.85	96.96	99.59	96.40
DDoS-TCP	99.21	95.34	95.88	99.54	95.61
Password	99.43	96.65	96.98	99.67	96.81
DDoS-HTTP	99.26	95.49	96.25	99.55	95.87
Uploading	99.36	96.46	96.43	99.65	96.44
Backdoor	99.31	96.50	95.64	99.66	96.07
XSS	99.30	96.09	96.09	99.61	96.09
Ransomware	99.33	95.45	92.06	99.75	93.73
Fingerpriniting	99.51	96.62	94.04	99.81	95.31
Average	**99.33**	**95.99**	**95.79**	**99.63**	**95.88**
TSPH (30%)					
Normal	99.29	96.32	95.68	99.64	96.00
DDoS-UDP	99.38	96.89	96.25	99.69	96.57
DDoS-ICMP	99.42	96.44	96.96	99.65	96.70
SQL injection	99.35	96.09	96.84	99.60	96.46
DDoS-TCP	99.32	95.77	96.49	99.59	96.13
Password	99.55	97.51	97.57	99.75	97.54
DDoS-HTTP	99.27	95.68	96.07	99.58	95.88
Uploading	99.30	96.25	95.93	99.63	96.09
Backdoor	99.33	96.23	96.42	99.62	96.33
XSS	99.42	96.36	97.01	99.65	96.68
Ransomware	99.41	94.70	93.71	99.72	94.20
Fingerpriniting	99.39	95.14	93.35	99.73	94.24
Average	**99.37**	**96.12**	**96.02**	**99.65**	**96.07**

Table 6. Cyberattack detection of ICSSADL-MHOA method on Edge-IIoT dataset.

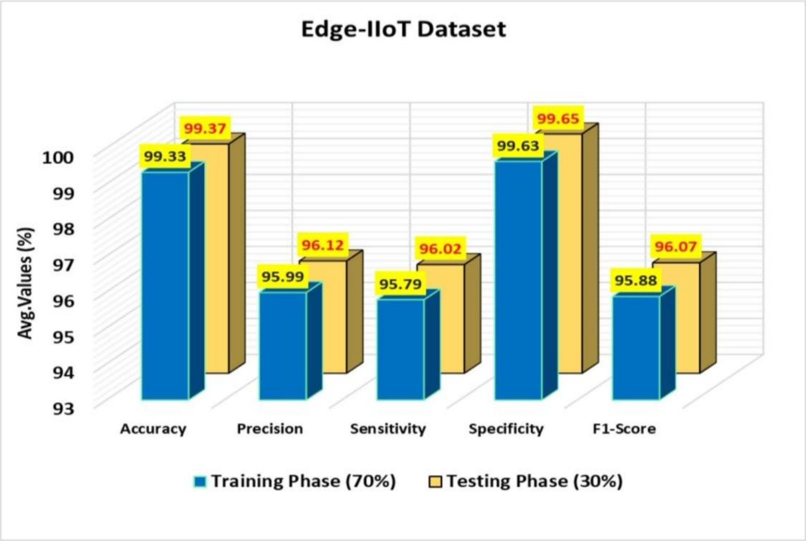


Fig. 13: Average of ICSSADL-MHOA method on Edge-IIoT dataset.

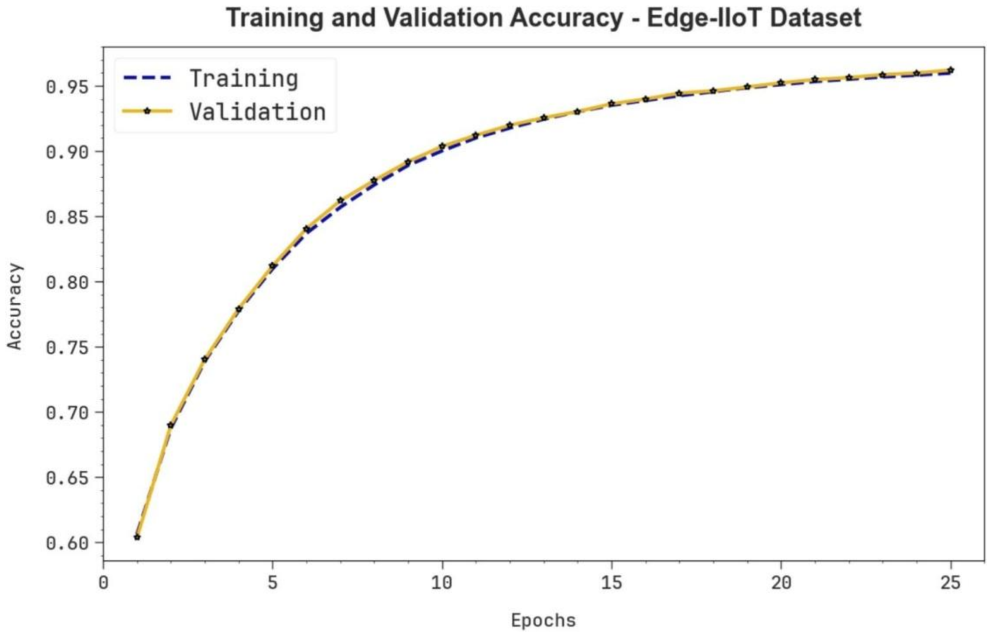


Fig. 14: Accu $_{y}$ curve of ICSS ADL-MHOA method on Edge-IIoT dataset.

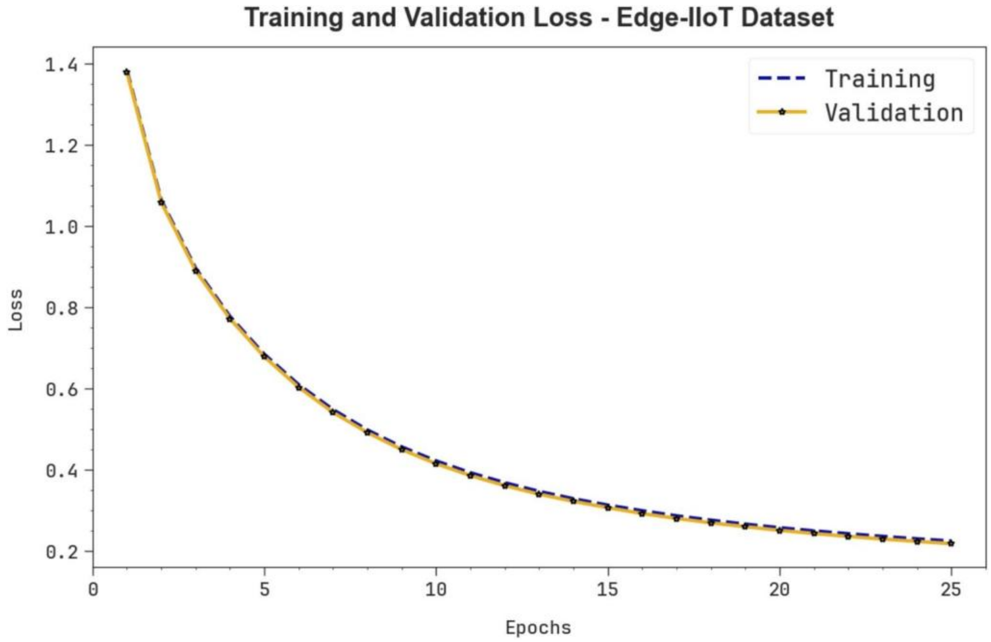


Fig. 15: Loss curve of ICSSADL-MHOA method on Edge-IIoT dataset.

Edge-IIoT Dataset				
Method	***Accu*$_y$**	***Prec*$_n$**	***Sens*$_y$**	***Spec*$_y$**
Shallow ANN	93.28	93.68	87.03	92.79
Isolated LSTM Model	98.19	93.66	88.86	92.85
CNN Mehtod	96.83	93.08	79.40	93.41

Random Forest	82.43	90.24	87.99	98.90
SVM Method	79.17	88.00	85.73	96.70
DNN Model	96.30	91.78	79.53	94.90
Inception Time	96.54	80.75	89.21	97.65
ICSSADL-MHOA	99.37	96.12	96.02	99.65

Table 7. Comparative analysis of ICSSADL-MHOA method on Edge-IIoT dataset[45–48].

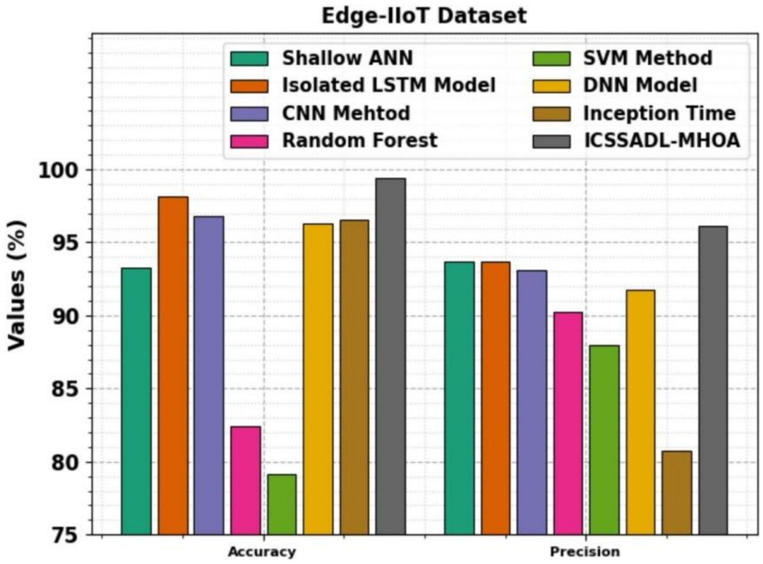


Fig. 16: Accu $_y$ and Prec $_n$ outcome of ICSSADL-MHOA method on Edge-IIoT dataset.

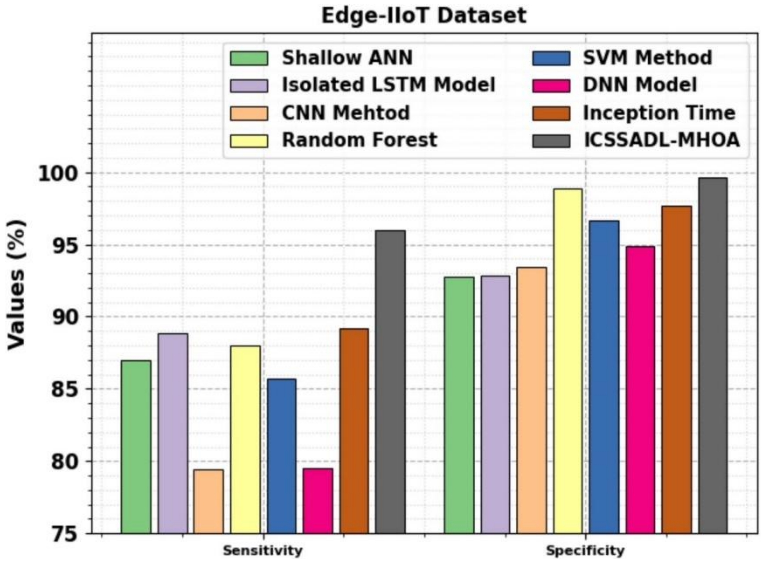


Fig. 17: Sens $_y$ and Spec $_y$ outcome of ICSSADL-MHOA method on Edge-IIoT dataset.

REFERENCES

1. Al-Haija, Q. A. & Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in iot
communication networks. Electronics 9, 2152 (2020).
2. Sarı, T. & GülesYigitol, H. K. B. Awareness and readiness of industry 4.0: The case of turkish manufacturing industry. Adv. Prod.
Eng. Manag. 15, 57–68 (2020).
3. Gupta, S., Sabitha, A. S. & Punhani, R. Cyber security threat intelligence using data mining techniques and artificial intelligence.
Int. J. Recent Technol. Eng. 8, 6133–6140 (2019).
4. Navandar, Pavan. " Unveiling the Power of Data Masking: Safeguarding Sensitive Information in the Digital Age" International Journal of Core Engineering & Management 5, no.6 (2019): 27-32.
5. Navandar, P. (2021). "Developing Advanced Fraud Prevention Techniques using Data Analytics and ERP Systems" Int J Sci Res, 10(5), 1326-1329.
6. Ameen, A. H., Mohammed, M. A. & Rashid, A. N. Enhancing security in IoMT: A blockchain-based cybersecurity framework for
machine learning-driven ECG signal classification. Fusion Pract. Appl. https://doi.org/10.54216/FPA.140117 (2024).
7. Smith, K. J., Dhillon, G. & Carter, L. User values and the development of a cybersecurity public policy for IoT. Int. J. Inf. Manag.
56, 102123 (2021).
8. Zhang, T., Zhao, Y., Jia, W. & Chen, M. Y. Collaborative algorithms that combine AI with IoT towards monitoring and control
system. Futur. Gener. Comput. Syst. 125, 677–686 (2021).
9. Al-Omari, M., Rawashdeh, M., Qutaishat, F. & AlshiraAbabneh, H. M. N. An intelligent tree-based intrusion detection model for
cyber security. J. Netw. Syst. Manag. 29, 20 (2021).
10. Navandar, Pavan. "Decoy Password Managers: Securing Against PII and Partial" ESP Journal of Engineering & Technology Advancements 4, no.2 (2024): 154-159. Doi: 10.56472/25832646/JETA-V4I2P126
11. Islam, U. et al. Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using
machine learning models. Sustainability 14, 8374 (2022).
12.Navandar, Pavan. "User Management Security: Best Practices and Strategies" European Journal of Advances in Engineering and Technology, 2021, 8(7):84-86
DOI: https://doi.org/10.5281/zenodo.11907037
13. HanEL-HasnonyCai, Y. I. M. W. Dragonfly algorithm with gated recurrent unit for cybersecurity in social networking. J. Cybersec.
Inform. Manag. 2, 75–85 (2019).
14. Imtiaz, N. et al. A deep learning-based approach for the detection of various internet of things intrusion attacks through optical
networks. Photonics. 12(1), 35 (2025).
15. Deshmukh, A. & Ravulakollu, K. An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity.
Technologies 12(10), 203 (2024).
16. Sattarpour, S., Barati, A. & Barati, H. EBIDS: Efficient BERT-based intrusion detection system in the network and application
layers of IoT. Clust. Comput. 28(2), 1–21 (2025).
17. Navandar "Empowering Organizations with SAP Governance, Risk, and Compliance (GRC) Solutions" Journal of Scientific and Engineering Research, 2022, 9(10):70-74.
18. Ragab, M. et al. Artificial intelligence driven cyberattack detection system using integration of deep belief network with convolution
neural network on industrial IoT. Alex. Eng. J. 110, 438–450 (2025).
19. Alsoufi, M. A. et al. Anomaly-based intrusion detection model using deep learning for IoT networks. Comput. Model. Eng. Sci.
141(1), 823–845 (2024).

20.Al-Neami, I. A., Hameed, Z. S. & Al-zubaydi, Z. A. Adaptive FPGA-based intrusion detection system for real-time internet of
things security. J. Intel. Syst. Net. Things https://doi.org/10.54216/JISIoT.140122 (2025).
21.Saravana Ram, R. & Gopi Saminathan, A. An intrusion detection system in wsn using an optimized self-attention-based progressive
generative adversarial network. IETE J. Res. https://doi.org/10.1080/03772063.2025.2452339 (2025).
22. Tewari, A. & Gupta, B. B. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Futur. Gener.
Comput. Syst. 108, 909–920 (2020).
23. Pavan Navandar, "Leveraging SAP GUI Scripting for Enhanced Automation" Journal of Artificial Intelligence Learning and Data Science , URF Publisher, 2022, https://doi.org/10.51219/JAIMLD/pavan-navandar/73
24. Santhanamari, P., Kathirgamam, V., Subramanian, L., Panneerselvam, T. & Chirakkal Radhakrishnan, R. Security enhancement in
5G networks by identifying attacks using optimized cosine convolutional neural network. Net. Technol. Lett. 8(2), e70003 (2025).
25. Zhao, G., Li, X. & Li, H. A trusted authentication scheme using semantic LSTM and blockchain in IoT access control system. Int.
J. Semant. Web Inform. Syst. (IJSWIS) 20(1), 1–27 (2024).
26. Mohamed, A. A., Al-Saleh, A., Sharma, S. K. & Tejani, G. G. Zero-day exploits detection with adaptive WavePCA-Autoencoder
(AWPA) adaptive hybrid exploit detection network (AHEDNet). Sci. Rep. 15(1), 4036 (2025).
27. Ashwini, K. & Nagasundara, K. B. An intelligent ransomware attack detection and classification using dual vision transformer with
mantis search split attention network. Comput. Electr. Eng. 119, 109509 (2024).
28. Zareh Farkhady, R., Majidzadeh, K., Masdari, M. & Ghaffari, A. 3DLBS-BCHO: A three-dimensional deep learning approach
based on branch splitter and binary chimp optimization for intrusion detection in IoT. Clust. Comput. 28(2), 83 (2025).
29. Perumal, E., Arulanthu, P., Ramachandran, R. and Singh, R. February. Enhanced Metaheuristics with Deep Learning Model for
Blockchain Assisted Cyber Security Solution in Internet of Things Environment. In 2024 Second, International Conference on
Emerging Trends in Information Technology and Engineering (ICETITE) 1–7 IEEE (2024).
30. Babitha, S. Efficient quantum inspired blockchain-based cyber security framework in IoT using deep learning and huristic
algorithms. Intell. Decis. Technol. 18(2), 1203–1232 (2024).
31. Lakicevic, B., Spalevic, Z., Volas, I., Jovanovic, L., Zivkovic, M., Zivkovic, T. and Bacanin, N. 2024 December. Artificial
Neural Networks with Soft Attention: Natural Language Processing for Phishing Email Detection Optimized with Modified
Metaheuristics. In International Conference on Advanced Network Technologies and Intelligent Computing 421–438 Cham: Springer
Nature Switzerland (2024).
32. Althobaiti, M. M. & Escorcia-Gutierrez, J. Weighted salp swarm algorithm with deep learning-powered cyber-threat detection for
robust network security. AIMS Math. 9(7), 17676–17695 (2024).
33. Yussif, A. F. S., Seini, T. & Adu, C. Improved tuna swarm optimization (ITSO) algorithm based on adaptive fitness-weight for global
optimization. Int. J. Electr. Eng. Appl. Sci. (IJEEAS) https://doi.org/10.54554/ijeeas.2024.7.02.011 (2024).