WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM
e-ISSN: 2788-5879 p-ISSN: 2788-5887

Hybrid Deep Learning Techniques for Improved Anomaly Detection in IoT Environments

Hanan Abbas Mohammed [1,*] **,Idress Mohammed Husien**[2]**,**

[1, 2] Department of Computer Science, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq

*Corresponding Author: Hanan Abbas Mohammed

DOI: https://doi.org/10.31185/wjcms.323
Received 20 November 2024; Accepted 21 December 2024; Available online 30 December 2024

ABSTRACT: The Internet of Things (IoT) is no longer limited to single personalities, but rather, it is a perceptions that has widely increased and spread in some applications or fields. The mechanism for communicating between IoT devices similarity works as traditional communication between hosts. However, the growing use of IoT has been gaining the interest of a growing number of attackers. Hence, a number of researchers are attempting to build an intrusion detection system utilizing machine learning and deep learning algorithms. In this work, a novel attack detection model is proposed by superimposing Whale Optimization Algorithm and Bidirectional Long Short-Term Memory (WB-LSTM) together. There are numerous deep learning competencies, but LSTM is one of the ones used to interpret big data or time series data. But, it is not easy to find what is the best weights for LSTMs in order to directly achieve performance. The LSTM results were 99.1%. Hence, in this work, we introduce the WOA-LSTM hybrid model, that utilizes WOA for finding the optimal weights for a network based on LSTM, and is used to detect the IoT attacks. The 99.98% was obtained from the WOA-LSTM hybrid model.

Keywords: CICIoT2023 Dataset, Feature scaling, IoT Security, Deep learning, LSTM Models, Whale optimization algorithm (WOA), Detect IoT Attacks.

1. INTRODUCTION

As the number of connected devices grows, so does the frequency of cyberattacks on these devices, particularly IoT botnets. The lack of human oversight during maintenance, vulnerabilities in sensors and cameras, and the fully automated nature of IoT devices all contribute to the exacerbation of these dangers. The expansion of IoT devices will further exacerbate the difficulty of malware detection, which is already a major concern [1-3]. The growing threat of IoT botnets necessitates collaboration between academic and industry researchers to develop more effective detection methods. Firewalls and other traditional intrusion detection systems are vulnerable to attacks. They might be mistaken if security rules aren't explicit or if they're not set up properly. Novel ML-based methods have evolved to address these issues. These algorithms learn complex concepts and patterns to help in intelligent decision-making. The effect of WOA's complicated random movements on convergence rates is the focus of this study. We propose new ways to examine and enhance the WOA's random movements to make the algorithm more efficient and to increase its convergence rates. To get over these problems, the proposed hybrid method makes use of a number of deep learning and machine learning strategies. The model uses cutting-edge algorithms and approaches to better detect botnet attacks on the IoT, providing robust security for IoT systems. Hybrid approaches effectively detect and classify botnet activity by combining advanced pattern recognition algorithms with cutting-edge data analysis techniques. The model efficiently and consistently identifies and counters attacks from IoT botnets using deep learning and machine learning capabilities.

In conclusion, Contributions: Development of a new realistic dataset for IoT attacks, utilizing a complex network of real IoT devices and involving IoT devices as both attackers and victims.

• Conducting, documenting, and gathering data from 33 attacks categorized into 7 classes targeting IoT devices, showcasing the replicability of these attacks.

• Assessment of machine and deep learning algorithm efficacy in classifying and detecting IoT network traffic as either malicious or benign using the CICIoT2023 dataset.

*Corresponding author: *stcm22005@uokirkuk.edu.iq*

2. RELATED WORK

The increasing prevalence of Internet of Things (IoT) devices has heightened the need for robust systems to detect and prevent cyberattacks. Numerous studies have explored improving IoT security using machine learning and deep learning techniques.

The paper examines the advantages and disadvantages of several IDS strategies, such as signature-based, anomaly-based, and hybrid systems. Machine learning (ML) approaches are essential in several application sectors, such as making predictions, identifying novel data structures, and estimating result functions.[4] Supervised learning involves training an artificial intelligence system to minimize a predetermined cost function while acquiring a mapping function from a dataset that includes input and output data [5]. If the algorithm's performance on the test set is consistent with its performance during training, it demonstrates successful generalization. Subsequently, the method is assessed using new data [6].

In unsupervised learning, an AI system is trained only using input data without any corresponding output data in the dataset [7]. By using this approach, you may explore captivating data structures and patterns. ML algorithms may effectively address application-specific difficulties by evaluating data that is divided into separate training and testing sets. There are two primary categories of ML algorithms: clustering and classification algorithms [8]. Classification algorithms analyze input characteristics and map them to the desired output using labelled data samples to construct prediction models [9]. A labelled dataset trains a classification model and instructs the model on identifying and categorising unfamiliar material.

Several machine learning and deep learning methods have recently been explored in intrusion detection systems (IDS) for the IoT and network security. Various research studies have used hybrid models that integrate different designs. A study [10] created and evaluated a hybrid CNN-LSTM model using the CIC-IDS2017 and CSE-CIC-IDS2018 datasets. The model had a remarkable accuracy rate of 98%. This paper primarily focused on intrusion detection systems that depend on machine learning. A study [11] This review aimed to examine DL techniques and continuing breakthroughs in approaches that may be used to produce enhanced attack detection models for IoT frameworks. It reviewed the applications of DL to IoT security and addressed the benefits and research gaps associated with each strategy. Another study [12], this review concluded that researchers are liberating themselves from Supervised Learning and moving toward Clustering and other algorithms, which gives the hope that IDS in the future will be able to detect more unknown and zero-day attacks also the percentage of utilizing hybrid algorithms has increased dramatically. A study [13] methodology integrates numerous machine learning models to predict heart disease. By capitalising on the merits of specific algorithms while addressing their drawbacks, this approach yields a predictive model that is more resilient. The findings of the research exhibit encouraging outcomes in heart disease prediction, attaining enhanced precision and dependability in contrast to discrete algorithms. Through the utilisation of ensemble learning, they successfully discerned predictive patterns that are linked to heart disease, thereby augmenting the capabilities of diagnostics.

Philipo, Adamu Gaston, et al. [14] used LSTM and multilayer perceptron (MLP) models for intrusion detection in IoT networks, and they also found a 0.98 accuracy rate. Ban, Yunfei, et al. [15] developed a distributed deep CNN-LSTM model to identify intrusions in IoT-based automobiles. This model attained an accuracy of 99.7% on the NSL-KDD dataset. This project aimed to enhance safety precautions for autos that depend on the Internet of Things. Altunay and Albayrak [16] used the UNSW-NB15 dataset to propose a hybrid CNN+LSTM approach for industrial IoT networks. Their solution attained an impressive accuracy rate of 93.21%. Their main objective was to enhance detecting capabilities in industrial IoT contexts. Zeeshan, Muhammad, et al. [17] demonstrated a 99.2% accuracy in detecting intrusions in IoT settings using the Bot-IoT dataset and employing LSTM. This study focused on using deep learning techniques to enhance security in IoT environments. Vu, Ly, et al. [18] In this paper, they propose a novel deep transfer learning (DTL) method that allows to learn from data collected from multiple IoT devices in which not all of them are labeled. Specifically, they develop a DTL model based on two AutoEncoders (AEs). The first AE (AE 1) is trained on the source datasets (source domains) in the supervised mode using the label information. The second AE (AE 2) is trained on the target datasets (target domains) unsupervised without label information. Stephen, Bliss Utibe-Abasi, et al.[19] conducted a study where they used a mixed-methods machine learning approach using K-Nearest Neighbours (KNN), Gradient Boosting (GB), and Support Vector Machines (SVM) on UCI Kaggle data. Their objective was to improve detection by using various machine-learning techniques. Hussein et al.[20] addressed the problem of computational efficiency in IoT-IDS by concentrating on feature selection algorithms to reduce time complexity. Using a combination of Support Vector Machines (SVM) and Random Forests (RF), the researchers successfully decreased the time required for calculation while achieving a commendable accuracy rate of 95% on IoT-IDS data. This research emphasises the ongoing pursuit of enhanced intrusion detection systems that safeguard networks and the Internet of Things. Researchers are increasingly exploring various combinations of convolutional neural networks (CNNs), long short-term memory (LSTMs), and traditional machine learning methods, leading to the growing popularity of hybrid models and deep learning architectures. The research covers a range of scenarios, including industrial IoT, IoT-enabled cars, and other types of IoT networks. The efficacy of these processes is shown by the consistently excellent precision rates, ranging from 93% to 99.7%. An increasing focus is on improving these systems' computing efficiency and optimization techniques to enhance their practical use.

Table 1: Recent study (2023-2024)

Ref.	Method	Model	Dataset	Contribution	Results	Accuracy
[21]	Clustering using DBSCAN enhanced by the Grey Wolf Optimizer.	DBSCAN-GWO.	N_BaIot datasets (six different IoT devices).	Automatic and adaptive tuning of DBSCAN's eps parameter for improved botnet detection.	DBSCAN-GWO outperformed traditional methods in botnet detection.	Up to 0.98 (98%) for the Philips B120N10 Baby Monitor dataset.
[22]	Ensemble learning with brute-force optimization.	NA	UCI Kaggle Cleveland dataset and IEEE Dataport dataset.	Improved heart disease prediction accuracy using ensemble soft voting and optimization techniques.	The proposed system consistently outperformed existing methods.	Achieved up to 98.21% accuracy with ensemble soft voting and 97.21% with brute-force optimization.
[23]	Few-Shot Meta Transfer Learning	Model-Agnostic Meta Learning (MAML)	• Mailing Dataset (9435 malware samples from 25 families) • Malevis Dataset (14,226 samples from 26 families, including benign samples)	Evaluated the effectiveness of meta-learning techniques for detecting previously unknown cyberattacks using different malware datasets.	• Good results on digital character recognition dataset. • Poor results on Malimg and Malevis datasets, indicating unreliability for malware detection.	92% on digital character recognition datasets; high validation loss on malware datasets
[24]	Machine Learning algorithms for DDoS attack detection.	K-Nearest Neighbors (KNN), Logistic Regression, Deep Neural Network (DNN).	CIC2023 IoT Dataset.	A comprehensive evaluation of ML algorithms for detecting DDoS attacks in IoT environments, achieving high detection accuracy and reduced false-positive rates.	High precision, recall, and F1 scores across models.	KNN accuracy: 0 (at n_neighbors=1); DNN accuracy: 0.9999; overall accuracy: 99.75% for the model discussed.
[25]	Machine Learning and Deep Learning techniques for anomaly detection.	• For ML: Random Forest (RF), LightGBM, XGBoost. • For DL: Long Short-Term Memory (LSTM), Convolutional Neural Network (CNN).	NSL-KDD, UNSW-NB15, CIC-IDS2017, CIC-IDS2018, IoT-23.	Improved detection of anomalies in IoT networks using advanced ML and DL models.	Achieved high accuracy and F1 scores compared to conventional models.	• NSL-KDD: 99.8%, F1 score: 0.998. • UNSW-NB15: 99.9%, F1 score: 0.999. • XGBoost: 99% accuracy.
[26]	Development of a BERT-	SecurityBERT.	Edge-IIoTset dataset.	Introduced a novel model that	he model effectively	98.2%.

	based model for cyber threat detection.			accurately classifies various cyber attack types while preserving privacy.	identifies fourteen distinct types of attacks.	
[27]	Deep learning-based detection system.	NA.	NA	Enhanced detection of network anomalies in cloud environments, outperforming traditional IDS methods.	High accuracy, recall, and precision in detecting network threats.	98.7%
[28]	Machine Learning-based multiclass anomaly detection and classification.	Random Forest (RF), Decision Tree (DT), Naive Bayes (NB), Support Vector Machine (SVM).	A dataset comprising sixteen indices and their pair combinations, totalling 136 pairs, with 4746 cases of various normal and anomaly events.	The study addresses the gap in multiclass classification for anomaly detection in power systems, demonstrating the effectiveness of selected ML classifiers.	The RF and DT classifiers achieved perfect precision, recall, and F-measure unity scores for the best-performing index pair.	100% accuracy for all types of anomaly events with the proposed RF and DT classifiers, outperforming existing techniques, which achieved a maximum of 99.9% accuracy
[29]	LSTM and Bi-LSTM models for soil moisture forecasting.	LSTM-based soil moisture forecasting model.	A dataset with 47,013 lines	Development of a forecasting model that improves prediction accuracy for soil moisture using advanced deep learning techniques.	The LSTM model achieved a training error of 0.03%, a test error of 0.08%, and an RMSE validation error of 1.057%. The Bi-LSTM model achieved a training error of 0.03%, a testing error of 0.04%, and a validation error of 0.783%.	The models demonstrated low training and validation errors, indicating strong performance in forecasting tasks.
[30]	Improved Bi-LSTM with an attention mechanism.	Attention-BiLSTM.	KDDcup99 dataset.	Enhanced detection accuracy and reduced false detection rates in network intrusion detection for IoT environments.	He proposed that the method outperformed comparison methods regarding false detection rate and detection accuracy.	94.98%

3. DATA DESCRIPTION

The below-mentioned research has introduced the dataset [31-34]. "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," Sensor (2023) – (submitted to Journal of Sensors). The present data contains different kinds of IoT intrusions. The categories of the IoT intrusions enlisted in the data are as follows: DDoS, Brute Force, Spoofing, DoS, Recon, Web-based, Mirai. Several subcategories are present in the data for each intrusion type in the IoT. The dataset contains 1191264 instances of networks for intrusions and 47 features for each. The dataset can be used to prepare the predictive model through which different kind of intrusive attacks can be detected. The data is also suitable for designing the IDS system.

Understanding and classifying these traffic types is crucial for cybersecurity professionals to strengthen network defences and enhance overall security. This comprehensive outlook on traffic behaviour is essential for training effective machine learning models to automate network threat detection and response. Moreover, creating a balanced dataset for testing and training using machine learning algorithms is crucial, given the imbalance found in the CICIoT2023 dataset between normal and attack traffic shown in Fig. 1., This balanced dataset will be essential for developing and testing optimization algorithms.

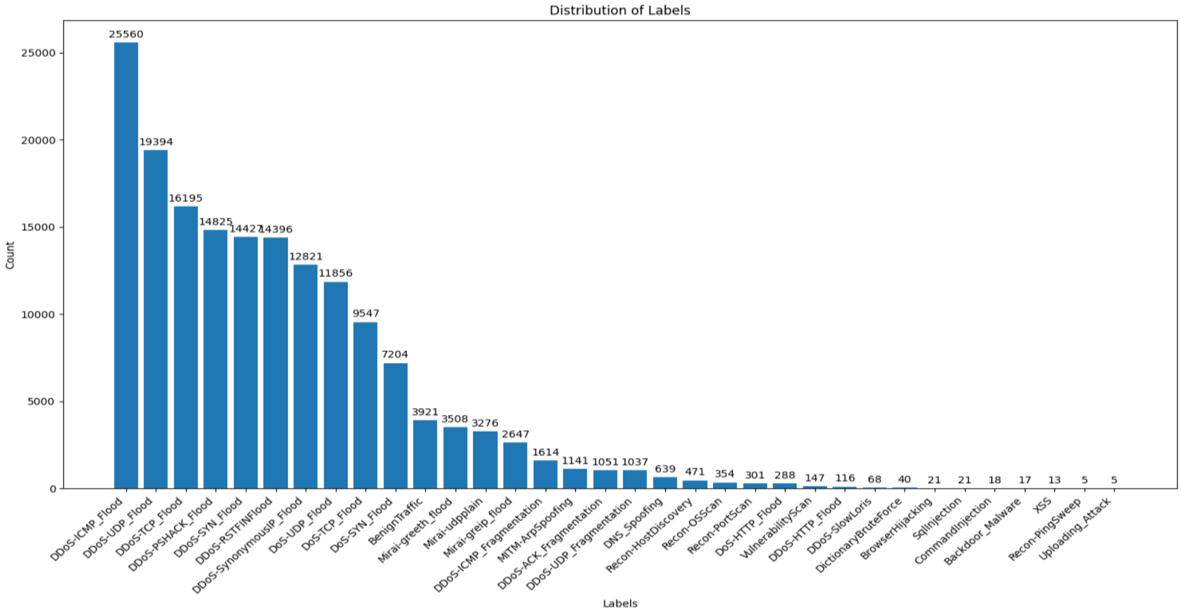

FIGURE 1. - First Features Group Histograms (Before balancing the dataset CICIoT 2023)[34]

Particularly in Internet of Things (IoT) settings, attackers use a broad array of tactics to exploit vulnerabilities in networks. The CICIoT2023 dataset includes several different types of traffic. By recognizing and understanding the various types of traffic, cybersecurity professionals may potentially fortify defenses, develop attack-specific detection systems, and enhance overall network security. The training of effective ML models to automate the identification and response to network threats requires this comprehensive view of traffic behavior. An imbalance between legal and malicious traffic was uncovered by extensive study of the dataset, which prompted us to build our own dataset. Only good for learning ML and DL algorithms and getting ready for exams.

Table 2. – Category records for binary classification, before and after sampling

Record type	Before sampling	After sampling
Normal	1003822	44753
Attacks	44753	44753

Binary classification is the task of labelling output into two groups. In our case, our binary classifiers should be able to decide whether a given record is an attack. To do that, we group label into two categories: Normal and Attack. Furthermore, to overcome unbalanced data issues, we used random sampling. Hence, we choose 44753 records for the normal category and 1003822 for the attacks category Table 2.

3.1 THE PURPOSE OF BALANCING THE DATASET

Balancing a dataset is a critical preprocessing step in machine learning, especially for applications where predictive accuracy across multiple classes is crucial, such as intrusion detection systems (IDS) for IoT security. The primary purpose of balancing a dataset is to prevent the model from being biased toward the majority class, thereby enhancing its ability to generalize well across all types of data it may encounter.

In many real-world datasets, such as the CICIoT2023 dataset, a significant imbalance is often observed where one class (e.g., "attack") vastly outnumbers other classes (e.g., "normal"). In such cases, machine learning models can develop a bias toward the majority class, as they have more examples from which to learn its characteristics. This means that although these models may excel at identifying the dominant class, they may struggle to recognize the minority class, which may be especially crucial in security-related contexts. It is crucial to transform an unbalanced dataset into a balanced one in order to train machine learning models successfully. Because of the critical nature of accurate predictions across several classes, this is especially true in domains such as intrusion detection systems and cybersecurity. By using under-sampling and over-sampling procedures until each class had about 44,753 occurrences, a new balanced dataset with 89,507 rows was constructed. This study aims to illustrate the process and reasoning behind this decision. The data is split evenly between normal operations and possible attacks.

It is crucial to transform an unbalanced dataset into a balanced one in order to train machine learning models successfully. Because of the critical nature of accurate predictions across several classes, this is especially true in domains such as intrusion detection systems and cybersecurity. This paper lays out the process and logic for creating a new balanced dataset. By using the under-sampling and oversampling processes to balance the numbers, 89,507 rows were created, with each class having about 44,753 occurrences. Figures 2 and 3 show that regular activities make up half of the data, while possible assault circumstances make up the other half.

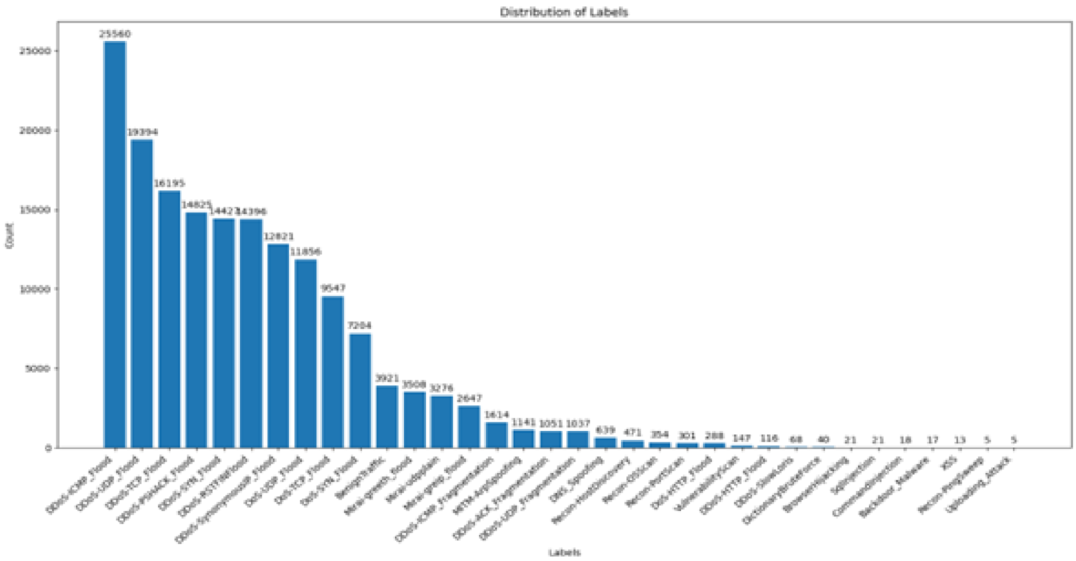

FIGURE 2. - Second Features Group Histograms (After balancing the CIC IoT 2023 dataset)

3.2 PREPROCESSING

It is crucial to pretreat data before using it in analysis or machine learning. Cleaning, converting, and otherwise making the data ready is part of data preparation for analysis and modeling. Standard methods include managing missing data, encoding categorical variables, extracting or selecting features, and removing duplicates. The most common ways to deal with missing data are row/column deletion, mean/median imputation, and interpolation. The purpose of the Duplicate Removal process is to lessen the occurrence of bias and duplicate data. The features are transformed and scaled using techniques such as min-max scaling, z-score normalization, and log transformation. category Variable Encoding is a technique for improving processing efficiency by numerically representing category variables. Finding and removing irrelevant characteristics is the job of feature selection and extraction. "Splitting" a dataset means dividing it into smaller parts that may be used at various stages of the process, such testing, validation, and training. Data augmentation might be useful if your training data is too homogeneous or lacks diversity. To mitigate the impact of out-of-the-ordinary findings, Outlier Detection and Handling eliminates data points with a large dispersion around the mean.

3.3 FEATURE SCALING

It is crucial to scale features while preparing data for AI and ML tasks so that algorithms can better assess the incoming data and make correct predictions. Better feature scaling methods and preprocessors are suggested as a means to enhance the model creation process in the research. Accurately scaling features enhances the output of the final model.

$$z = \frac{(x - \mu)}{\sigma} \qquad (1)$$

Where:

- x is the original value of a feature.
- μ is the mean of the feature values.
- σ is the standard deviation of the feature values.

Feature scaling and encoding are two essential preprocessing procedures in machine learning that prepare datasets for model training. A feature scaling technique provides equal representation of all features and minimises the impact of larger scales on learning. Commonly, this is achieved using techniques such as Standard Scaler. The process of feature scaling involves converting numerical characteristics to possess a mean value of zero and a standard deviation of one. Encoding renders categorical data suitable for algorithms that need numerical input, such as Label Encoder, to convert classification variables into numerical representation. These techniques aim to standardize and refine datasets to enhance the efficiency and accuracy of machine learning models in learning from them.

4. LSTM DEEP LEARNING ALGORITHM

Long Short-Term Memory (LSTM) RNNs have a single application case: cyberattack detection. Since present models depend on supervised methodologies, processing delays for large-scale attacks are not considered. This is a problem with real-time detection. Long short-term memory (LSTM) models may learn valuable information from sequence data, which is important in cybersecurity. Their extraordinary memory capacity allows them to thrive when presented with sequences as input. Since this is the case, LSTMs might be helpful for dealing with security issues in IoT networks. The use of LSTM models is crucial in addressing the increasing complexity of IoT systems.

We will examine the mathematical definition of LSTM next. Long short-term memory (LSTM) networks include a number of gates, like as:

- Forget gate: deciding what information should be thrown away or kept.
- Input gate: deciding which values for the different components should be updated.
- Output gate: deciding the actual output based on the input and the memory.

These gates can be implemented with any value between 0 and 1, and can be done using the sigmoid function. The sigmoid function allows us to calculate values between 0 and 1. One example of the sigmoid function is given below.

$$\sigma(X) = 1/\left(1 + e^{\wedge}\,(-X)\right)$$

Mathematically, the gates of the LSTM are given by the following equations:

$$ft = \sigma(Wf.[ht - 1; Xt] + bf) \qquad (2)$$
$$it = \sigma(Wi.[ht - 1; Xt] + bi) \qquad (3)$$
$$ot = \sigma(Wo.[ht - 1; Xt] + bo) \qquad (4)$$

Where ft, it, and not are the forget, input, and output gates. The formulation to compute the LSTM activations in the next time step is given by:

$$\tilde{c}t = tanh(Wc.[ht - 1, Xt] + bc) \qquad (5)$$
$$ct = ft * ct - 1 + it * \tilde{c}t \qquad (6)$$
$$ht = ot * tanh(ct) \qquad (7)$$

Here, xt is the input at the time-step 't', ht is the output at time step 't', and ct is the cell state at time step 't'. Moreover, + * denote point-wise multiplication. The W's and b's in the equations represent the weight matrices and biases. The activation functions in the equations could be ReLU, tanh, or simply a linear activation function (i.e., f(x) = x). The LSTM network is trained using the back-propagation training strategy. Given the error at time 't', it updates the error of train the network with gradient descent. This makes it straightforward to use the implemented algorithm and to transfer it between different libraries or software.

4.1 BI-DIRECTION LONG SHORT-TERM MEMORY(BILSTM ARCHITECTURE)

The following section outlines the structure and properties of the basic BLSTM algorithm. The bidirectional LSTM (BLSTM) is a modification of Recurrent Neural Networks that expands upon the traditional LSTM model. It examines sequences in both forward and backward directions, incorporating contextual information from preceding and subsequent elements. This dual approach enhances the model's ability to understand and represent complex relationships in sequential data [35] as shown in Fig 3. Below are some definitions related to the BLSTM algorithm [36]:

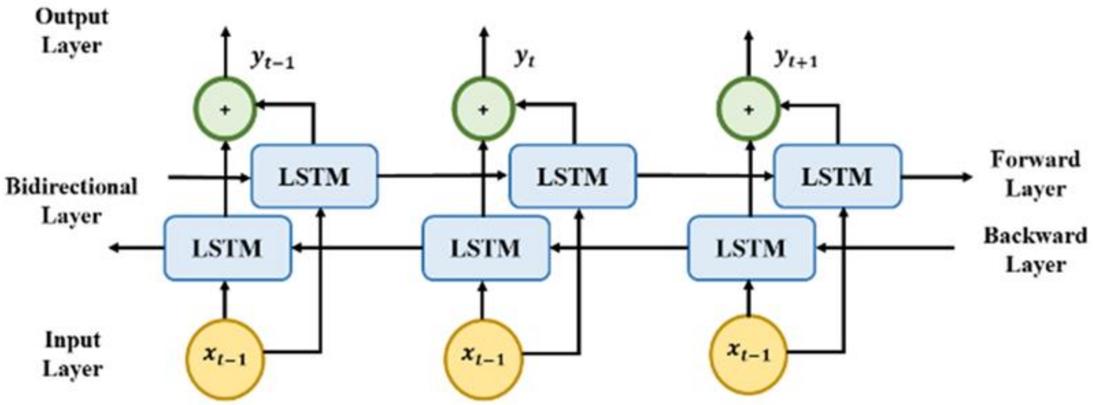

FIGURE 3. - Bidirectional –LSTM Model [34]

- Number of Units/Neurons: Controls the model's learning capacity.
- Dropout Rate: Prevents overfitting by randomly dropping units during training.
- Sequence Length: Defines the length of input sequences processed.
- Batch Size: Number of samples processed at once during training.
- Learning Rate: Dictates how fast the model updates weights.
- Activation Functions: Introduces non-linearity in LSTM cells.
- Number of Layers: Determines the depth of the model by stacking BLSTM layers.
- Optimizer: Algorithm that adjusts weights during training.
- Bidirectional Mode: Processes data in both forward and reverse directions for comprehensive context.

4.2 THE PROPOSED BILSTM WITH WHALE OPTIMIZATION ALGORITHM

An approach to identifying IoT assaults is shown here using bidirectional-LSTM fine-tuned using the Whale optimization algorithm (Fig. 4). The Whale Optimization Algorithm enhances the precision of data classification by determining the optimal values for the BiLSTM parameters, which include the number of units and the dropout rate. These values are then used for training and testing purposes. By determining the optimal number of units that strike a balance between complexity and performance, WOA helps to avoid overfitting and effectively capture important sequence patterns.

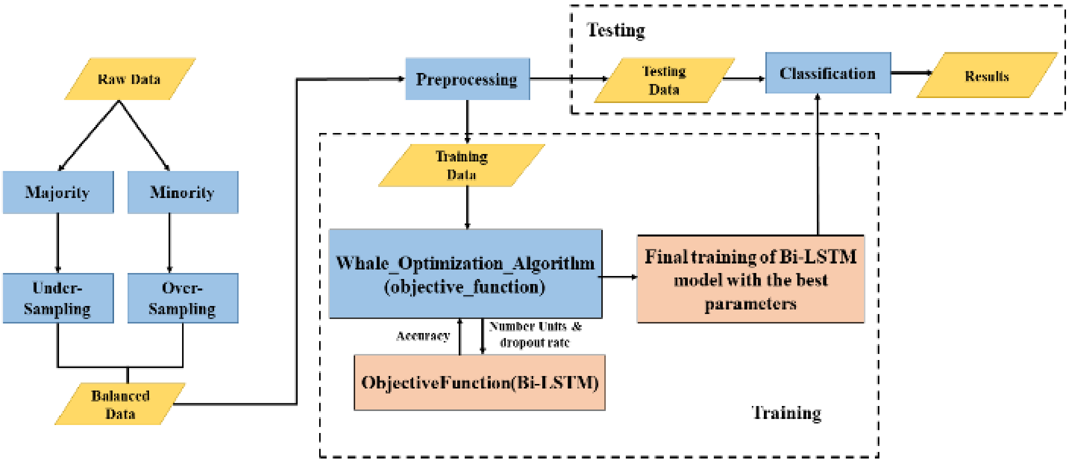
Testing
Raw Data
Preprocessing
Testing Data
Classification
Results
Majority
Minority
Training Data
Under-Sampling
Over-Sampling
Whale_Optimization_Algorithm (objective_function)
Final training of Bi-LSTM model with the best parameters
Accuracy
Number Units & dropout rate
ObjectiveFunction(Bi-LSTM)
Balanced Data
Training

FIGURE 4. -BiLSTM-WOA Model Framework.

Alternatively, the dropout rate controls the amount of units that are "dropped" at random during training to prevent overfitting. In order to get optimal results, WOA experiments with different dropout rates and applies the one that enhances generalizability while minimizing performance losses. This, in conjunction with the model's ability to identify bidirectional sequence relationships, makes for a more robust BiLSTM model that avoids overfitting and keeps crucial data intact throughout training. The dataset must be balanced before the proposed model can be used. Choosing a bigger minority sample and a smaller majority sample is one approach. This mechanism's capacity to encourage consistent learning across all courses leads to improved accuracy and generalizability.

5. WHALE OPTIMIZATION ALGORITHM (WOA)

The Whale Optimization Algorithm (WOA) model is motivated by the mechanics of searching for food. WOA contains the movement mechanism of the three types of whales during foraging. WOA was selected over other Metaheuristic Optimization models due to its comprehensive search approach, better capacity for local search, acceleration coefficients, and the calculations used as shown in Fig 4 and Algorithm 1.

Algorithm 1: Whale Optimization Algorithm

Input: Random Initialization of Feature Subsets.

Output: The position of the best whale.

```
1.  Calculate the value of the parameter a based on the current iteration.

2.  For each whale in the population:

            If hv<0.5:
                If |A|<1:
                        Update the whale's position based on the shrinking encircling mechanism |D|.
        If |A|≥1:
          Randomly select another whale SWr from the population.
          Update the whale's position based on the randomly selected whale SWr.
        If h ≥ 0.5:
        Update the whale's position based on the spiral updating position method (attacking prey in a spiral path).

      End for each whale.

3.  Fitness Evaluation:

4.  End of the Main Loop.
```

In the Whale Optimization Algorithm, the variables used are:

- SW: The best whale found so far, representing the solution with the highest fitness value.
- t{max}: The maximum number of iterations or the stopping criterion for the algorithm.
- a: A coefficient that decreases linearly from 2 to 0 throughout iterations. It controls the balance between exploration and exploitation.
- h: A random number in the range [0, 1]. It determines whether the whale should shrink its encircling mechanism or move towards a randomly selected whale (search agent).
- A: A vector calculated based on aaa that determines the distance between the whale's current position and the position of the best whale or a randomly selected whale.
- SWr: A randomly selected whale from the population. Used when |A|≥1 to diversify the search process.
- D: The distance between the whale's current position and the prey (either the best solution SW or another whale SWr).

The application area of WOA is vast, including data mining, cost optimization, clustering, electric vehicles, energy management systems, optical communication, permutation flow-shop scheduling, power supply systems, swarm and evolutionary algorithms, and many more. The WOA algorithm has beneficial characteristics like simplicity, minimal controllable factors, and strong search exploiter. In the first attack-shot, it is useful for formulating WOA rules in LINEED. By discussing the behavior of various WOA rules and their mixture, the proposal testifies to the significance of using two WOA operators: a chase communicator and a feasting communicator. Scaling Move is a step in which the span is decreased, and search in the direction of prey should now commence (Move = Position of a winner "p" - [Xifft, where Xi is the search of the whale i on a variable"). This process is done using the next equation. The current adjustable dimensions complete the whale or seeker motion. The movement of the hunter should be restricted to this range. The motion of the prey/hunter can be limited to the bounds of the issue by the given material. Nevertheless, if the whale is closest to the boundaries of the quest, as shown in Fig 5.

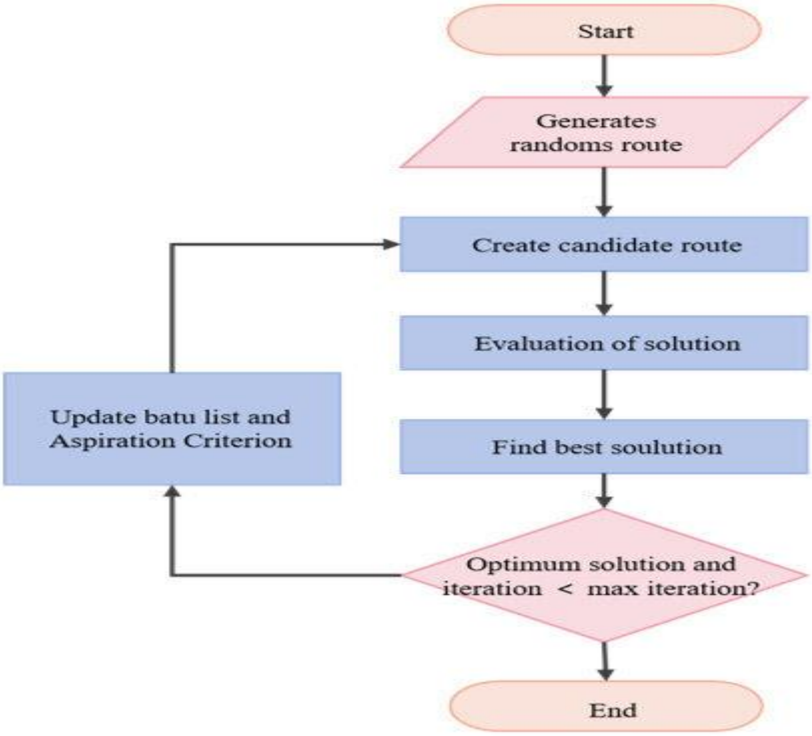

FIGURE 5. **-WOA feature selection algorithm flowchart [37]**

6. PROPOSED METHOLOGY

IoT attack data involves complex, time-dependent patterns and evolving data. Machine learning often struggles with IoT attack data because it may not effectively capture the intricate, time-sensitive patterns and dynamic changes inherent in the data [38-40]. This paper proposes the detection of IoT attacks with deep learning techniques. The employed deep learning algorithm is BLSTM, optimized using the WOA algorithm. The Whale Optimization Algorithm determines the optimal number of BLSTM units and the dropout rate. Conventionally, the parameters for the number of neurons in BLSTM and the dropout rate are determined manually or through trial and error, which is impractical for real-world IoT attack detection methodologies. Each data collection necessitates distinct parameter values for optimal detection accuracy. Subsequently, we shall examine the phases of the model in depth.

6.1 ENHANCED WHALE OPTIMIZATION ALGORITHM(EWOA)

Researchers have developed an improved algorithm called (EWOA) based on the classical Whale Optimization Algorithm (WOA) to enhance the computational efficiency and detection performance of IoT attack detection. The decision agent's learning mechanism for predicting cyber-attacks is categorized as Learn New Behavior (LNB), Reinforce Good Behavior (RGB), and Punish the Bad Behavior (PBB). Within Reinforce Good Behavior (RGB), the decision agent reinforces "good" behaviors for each attacker to enhance attack effectiveness. In contrast, in Punish the Bad Behavior (PBB), the decision-agent conducts attacks likely to be ineffective. The infection amplitude, or the intensity of an attack, is determined by the number of packets from an attacker over a given time interval. The parameter search space includes the magnitudes of outlier infection values, η ∈ <0, η max>, which defines the potential bounds of infection levels. The value of η after the execution of DRL, to discover a zero-day attack, is used by a dedicated IoTDI-IDS to block or modify an action to manage infected devices. During inference time, E1 searches for attacks that could bypass existing rule-set network detectors, and alerts are raised upon successful penetration. The Decision-agent for cyber-attack prediction also recommends sufficient computation resources for ML model training. Use-cases across various conditions (e.g. bots, Normal, and DDoS attack behaviors) demonstrate that EWA significantly outperforms detection methods. A variant of E-WOA adopting LSTM does not significantly improve, despite incorporating long-term dependencies as shown in Fig 6.

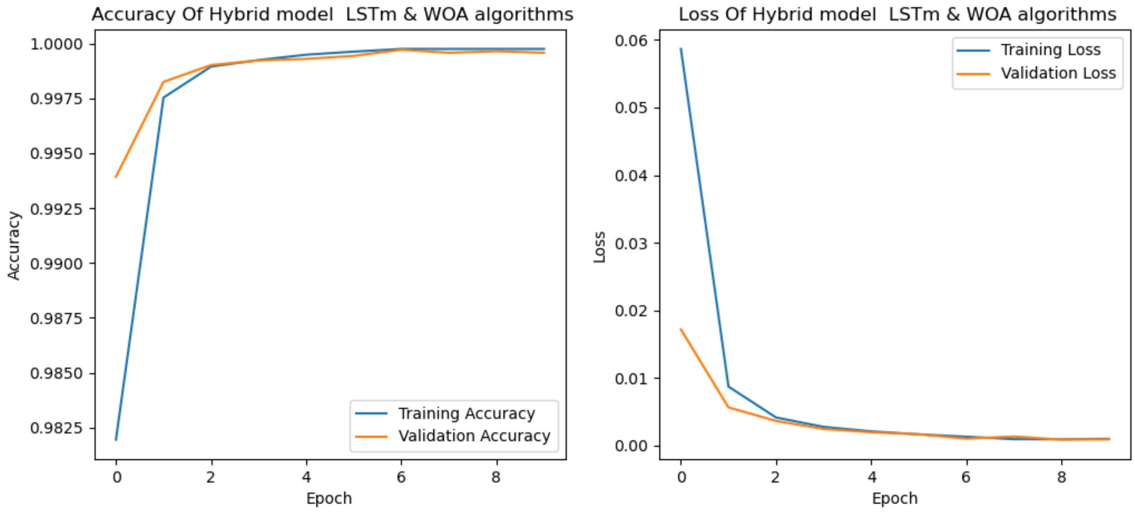

FIGURE 6. -Data training results using the proposed model for the dataset CICIoT2023.

6.2 MODEL EVALUATION METRICS

The performance of classification models in text analysis can be evaluated using precision, recall, F1-score, and accuracy. Precision reflects the ability to retrieve relevant instances, while recall represents the ability to retrieve all relevant instances. F1-score balances precision and recall. Accuracy measures the ratio of correctly predicted instances to all instances. Precision measures the relevance of selected items, while recall measures the selection of relevant items .

Accuracy indicates how many predicted instances are correct. It is calculated using the formula:
Accuracy = (TP + TN) / (TP + TN + FP + FN).

$$Accurcy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (8)$$

$$precison = \frac{TP}{TP + FP} \qquad (9)$$

$$Recall = \frac{TP}{TP + FN} \qquad (10)$$

$$F_1 = \frac{2TP}{2TP + FP + FN} \qquad (11)$$

6.3 MODEL TRAINING AND TESTING

This paper uses the hybrid Whale Optimization Algorithm and Long Short-Term Memory (WOA-LSTM) deep learning model for detecting Data-Link (DoS and MITM) in IoT-based wireless sensor network applications. First, we divided the data into 80% for training and 20% for model testing. For the model's performance evaluation, this model was tested and validated using five commonly used performance indicators: False Alarm (FA), Miss-Detection (MD), Precision (P), Sensitivity (SN), and F1 score. The SN, P, and F1 scores for DDoS detection are 98%, 92%, and 95%, respectively. In DoS detection (DoS-DDoS combined), the SN, P, and F1 scores are 99%, 95%, and 97%, respectively. Unfortunately, to our knowledge, there are no comparison data and similar hybrid IoT-LSTM models for integrated DoS and DDoS attacks. However, if we compare LSTM and hybrid-LSTM scores with hybrid and individual scores in the literature review.

The Training Process: The number given is divided into 80% of training data for both target model and evaluation purposes. The original accuracy of DoS and DDoS attacks is 99.6%. After anomaly detection, however, it decreases to 99.2%.

Testing Protocols: The remaining 20% of the data is used for an integrated test. Although the novelty results show potential for maintaining the original accuracy, these results might not reflect future cyber-attacks or their new trends.

Experiment Results: Thus, future research aims to continuously update and enhance the proposed model with new datasets and their anomaly patterns. The attack detection range is restricted, and the accuracy is affected. As can be observed, the changes in the original accuracy in detecting DoS and DDoS attacks were recorded and affected by anomaly detection. Consequently, the DoS accuracy slightly decreased from 99.6% to 99.2% when combined with the DoS and DDoS data.

6.4 MODEL EVALUATION

A hybrid model integrating Long Short-Term Memory (LSTM) networks with the Whale Optimization Algorithm (WOA) was evaluated using the Intrusion Detection Evaluation Dataset (CIC-IDS2017). Precision, accuracy, recall, and F1-score were some of the measures used to evaluate the model's performance. The WOA improves the model's optimization process by quickly searching for optimum parameters. At the same time, the LSTM component captures temporal relationships and sequential patterns in incursion data[31]. By combining them, we hope to increase the efficiency of model training by capitalizing on the advantages of both techniques. It is clear from the assessment findings that the suggested model works well as shown in Fig 7.

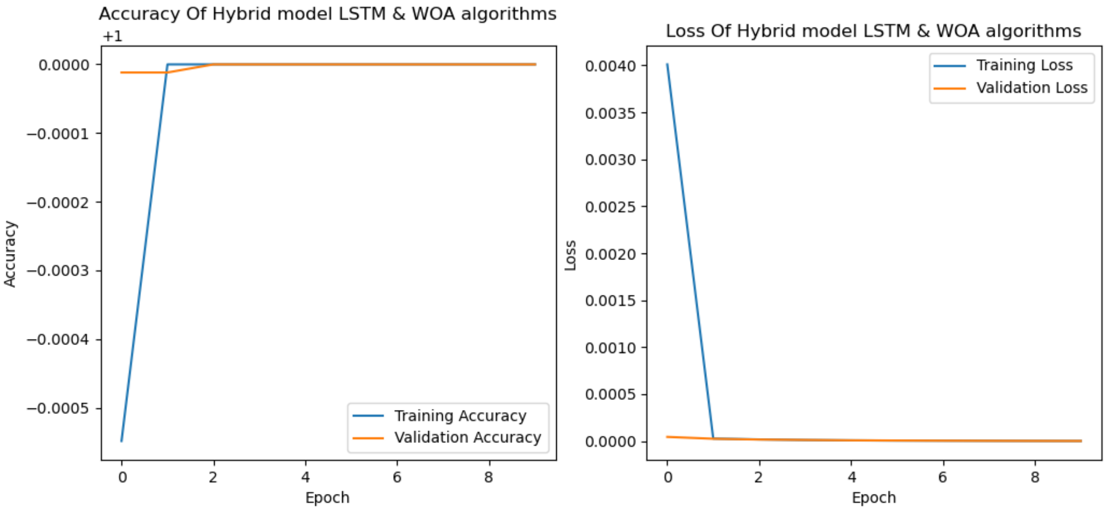

FIGURE 7. - Data training results using the proposed model for the dataset CIC-IDS2017.

7. EXPERIMENTAL RESULTS AND DISCUSSION

With the new hybrid model that combines the LSTM and EWOA deep learning algorithms, identifying threats on the Internet of Things (IoT) has never been simpler. This approach aims to optimize model selection for all qualities by feeding data from the WOA search technique into three distinct LSTM models. The hybrid model integrates offline and online training and testing, with a focus on the blocked and blockage loss function, to choose outlier symbols and alternative inputs for the LSTM and WOA-LSTM models. The WOA algorithm finds the best answers with the least amount of computing effort by simplifying the process and making the parameters less clear. The Long Short-Term Memory (LSTM) architecture integrates three main components—the candidate activation function, the memory cell, and the forgetting activation function—to address training loads and scalability issues. By integrating advanced training processes with predictions made by sources other than AI, the hybrid model enhances the training capabilities of deep learning. To choose the most suitable candidate function topology for LSTM development, it uses WOA. The model's efficiency and robustness are demonstrated by metrics for its performance in different class distribution scenarios: in the 40-60 distribution, it hit 0.91 precision, 0.98 recall, 0.94 F1-score, and 0.98 accuracy; in the 30-70 distribution, it hit 0.97 precision, 0.91 recall, 0.94 F1-score, and 0.97 accuracy; and in the 20-80 distribution, it hit 0.94 precision, 0.94 recall, 0.94 F1-score, and 0.99 accuracy. The results demonstrate that the model maintains its equilibrium and fares adequately when the distributions of the classes are altered. Maximizing this model's potential requires tailoring it to meet the accuracy and recall requirements of individual applications and conducting thorough evaluations using additional metrics like ROC-AUC and precision-recall curves. These additional metrics offer more detailed insights into performance, as shown in Table 3.

Table 3: Training results for the proposed model within multiple divisions

Class Distribution	Precision%	Recall%	F1-Score%	Accuracy%
40-60	0.91	0.98	0.94	0.98
30-70	0.97	0.91	0.94	0.97
20-80	0.94	0.94	0.94	0.99

8. CONCLUSION

This study introduced a new approach to improve the detection of attacks on Internet of Things devices. The method makes use of a hybrid model of two deep learning algorithms, one of which is the Enhanced Whale Optimization Algorithm (EWOA) and the other long short-term memory (LSTM). The goal of combining the WOA search technique with each of the three LSTM models is to identify the attribute-specific model with the highest implementation efficiency. Using the blocked and blockage loss function to choose outlier symbols and alternate inputs for the LSTM and WOA-LSTM models, the proposed hybrid technique combines online testing and training with offline training. The WOA approach has many applications, one of which is finding great solutions with reduced computational costs and ambiguous parameters. Regardless of the ratio, the hybrid model's performance results show that it effectively identifies attacks with excellent accuracy (0.91-0.98), recall (0.91-0.98), and F1-score (0.94-0.94). To sum up, the proposed hybrid model handles the complex and dynamic data prevalent in IoT environments with ease and effectively identifies risks, making it a promising choice for improving IoT security. These findings are critical for developing IoT security solutions that will last.

Funding

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] S. U. Qureshi, J. He, S. Tunio, N. Zhu, A. Nazir, A. Wajahat, ... & A. Wadud, “Systematic review of deep learning solutions for malware detection and forensic analysis in IoT,” *Journal of King Saud University-Computer and Information Sciences*, vol. 102164, 2024, doi: 10.1016/j.jksuci.2024.102164.

[2] A. Goni, M. U. F. Jahangir, & R. R. Chowdhury, “A study on cyber security: Analyzing current threats, navigating complexities, and implementing prevention strategies,” *International Journal of Research and Scientific Innovation*, vol. 10, no. 12, pp. 507-522, 2024, doi: unavailable.

[3] F. N. U. Jimmy, “Cyber security vulnerabilities and remediation through cloud security tools,” *Journal of Artificial Intelligence General Science (JAIGS)*, vol. 2, no. 1, pp. 129-171, 2024, doi: unavailable.

[4] H. Sun, H. V. Burton, & H. Huang, “Machine learning applications for building structural design and performance assessment: State-of-the-art review,” *Journal of Building Engineering*, vol. 33, p. 101816, 2021, doi: 10.1016/j.jobe.2020.101816.

[5] N. Burkart, & M. F. Huber, “A survey on the explainability of supervised machine learning,”*Journal of Artificial Intelligence Research*, vol. 70, pp. 245-317, 2021, doi: 10.1613/jair.1.12228.

[6] G. C. Cawley, & N. L. Talbot, “On over-fitting in model selection and subsequent selection bias in performance evaluation,” *The Journal of Machine Learning Research*, vol. 11, pp. 2079-2107, 2010, doi: unavailable.

[7] J. Wang, & F. Biljecki, “Unsupervised machine learning in urban studies: A systematic review of applications,” *Cities*, vol. 129, p. 103925, 2022, doi: 10.1016/j.cities.2022.103925.

[8] N. K. Neeraj, & V. Maurya, “A review on machine learning (feature selection, classification and clustering) approaches of big data mining in different areas of research,” *Journal of Critical Reviews*, vol. 7, no. 19, pp. 2610-2626, 2020, doi: unavailable.

[9] P. C. Sen, M. Hajra, & M. Ghosh, “Supervised classification algorithms in machine learning: A survey and review,” in *Emerging Technology in Modelling and Graphics: Proceedings of IEM Graph 2018,* Singapore: Springer, 2020, pp. 99-111, doi: 10.1007/978-981-13-7403-6_10.

[10] I. A. Abdulmajeed & I. M. Husien, “MLIDS22- IDS Design by Applying Hybrid CNN-LSTM Model on Mixed-Datasets,” *Informatica (Slovenia)*, vol. 46, no. 8, pp. 121–134, 2022, doi: 10.31449/inf.v46i8.4348.

[11] H. A. Mohammad, & I. M. Husien, “Machine Learning Algorithms and for robust IoT attack detection: A review,” *Informatica*, vol. 48, no. 12, pp. 55-64, 2024, doi: unavailable.

[12] I. A. Abdulmajeed & I. M. Husien, “Machine Learning Algorithms and Datasets for Modern IDS Design,” in *Proceedings - 2022 IEEE International Conference on Cybernetics and Computational Intelligence*, CyberneticsCom 2022, 2022, doi: 10.1109/CyberneticsCom55287.2022.9865255.

[13] M. Ahmed, & I. Husien, “Heart Disease Prediction Using Hybrid Machine Learning: A Brief Review,”*Journal of Robotics and Control (JRC)*, vol. 5, no. 3, pp. 884-892, 2024, doi: unavailable.

[14] A. G. Philipo, D. S. Sarwatt, J. Ding, M. Daneshmand, & H. Ning, “Cyberbullying detection: Exploring datasets, technologies, and approaches on social media platforms,” *arXiv preprint*, arXiv:2407.12154, 2024, doi: unavailable.

[15] Y. Ban, D. Zhang, Q. He, & Q. Shen, “APSO-CNN-SE: An adaptive convolutional neural network approach for IoT intrusion detection,” *Computers, Materials & Continua*, vol. 81, no. 1, 2024, doi: unavailable.

[16] H. C. Altunay, & Z. Albayrak, “A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks,” *Engineering Science and Technology, an International Journal*, vol. 38, p. 101322, 2023, doi: 10.1016/j.jestch.2022.101322.

[17] M. Zeeshan, Q. Riaz, M. A. Bilal, M. K. Shahzad, H. Jabeen, S. A. Haider, & A. Rahim, “Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and Bot-IoT datasets,” *IEEE Access*, vol. 10, pp. 2269-2283, 2021, doi: 10.1109/ACCESS.2021.3053957.

[18] Vu, L., Nguyen, Q. U., Nguyen, D. N., Hoang, D. T., & Dutkiewicz, E. (2020). Deep transfer learning for IoT attack detection. IEEE Access, 8, 107335-107344.

[19] B. U. A. Stephen, B. C. Uzoewulu, P. M. Asuquo, & S. Ozuomba, “Diabetes and hypertension mobile health systems: A review of general challenges and advancements,” *Journal of Engineering and Applied Science*, vol. 70, no. 1, p. 78, 2023, doi: unavailable.

[20] A. Y. Hussein, P. Falcarin, & A. T. Sadiq, “Enhancement performance of random forest algorithm via one hot encoding for IoT IDS,” *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 3, pp. 579-591, 2021, doi: unavailable.

[21] D. H. Mustafa, & I. M. Husien, “Adaptive DBSCAN with Grey Wolf Optimizer for Botnet Detection,” *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 409–421, 2023, doi: 10.22266/ijies2023.0831.33.

[22] M. Ahmed, & I. Husien, “Hybrid Machine Learning Approach for Accurate Heart Disease Prediction,” *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 4, pp. 728–737, 2024, doi: 10.22266/IJIES2024.0831.55.

[23] T. Ige, C. Kiekintveld, A. Piplai, A. Wagler, O. Kolade, & B. Matti, “Towards an in-depth evaluation of the performance, suitability and plausibility of few-shot meta transfer learning on an unknown out-of-distribution cyber-attack detection,” 2024, doi: unavailable.

[24] A. Berqia, H. Bouijij, A. Merimi, & A. Ouaggane, “Detecting DDoS attacks using machine learning in IoT environment,” in *2024 International Conference on Intelligent Systems and Computer Vision (ISCV)*, IEEE, 2024, pp. 1-8, doi: 10.1109/ISCV.2024.9456205.

[25] S. H. Rafique, A. Abdallah, N. S. Musa, & T. Murugan, “Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends,” *Sensors*, vol. 24, no. 6, p. 1968, 2024, doi: 10.3390/s24061968.

[26] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, & N. S. Thandi, “Revolutionizing cyber threat detection with large language models: A privacy-preserving BERT-based lightweight model for IoT/IIoT devices,” *IEEE Access*, 2024, doi: unavailable.

[27] Y. Lin, “Enhanced Detection of Anomalous Network Behavior in Cloud-Driven Big Data Systems Using Deep Learning Models,” *Journal of Theory and Practice of Engineering Science*, vol. 4, no. 08, pp. 1-11, 2024, doi: unavailable.

[28] S. Chandio, J. A. Laghari, M. A. Bhayo, M. A. Koondhar, Y. S. Kim, B. B. Graba, and E. Touti, “Machine Learning-Based Multiclass Anomaly Detection and Classification in Hybrid Active Distribution Networks,” *IEEE Access,* 2024, doi: unavailable.

[29] P. Suebsombut, A. Sekhari, P. Sureephong, A. Belhi, and A. Bouras, "Field data forecasting using LSTM and Bi-LSTM approaches," *Applied Sciences*, vol. 11, no. 24, p. 11820, 2021, doi: 10.3390/app112411820.

[30] X. Fan and R. Yang, "A network intrusion detection method based on improved Bi-LSTM in Internet of Things environment," *International Journal of Information Technologies and Systems Approach (IJITSA),* vol. 16, no. 3, pp. 1–14, 2023, doi: 10.4018/IJITSA.321738.

[31] B. Kaur, S. Dadkhah, F. Shoeleh, E. C. P. Neto, P. Xiong, S. Iqbal, ... and A. A. Ghorbani, “Internet of Things (IoT) Security Dataset Evolution: Challenges and Future Directions,” *Internet of Things*, vol. 22, p. 100780, 2023, doi: 10.1016/j.iot.2023.100780.

[32] A. Zohourian, S. Dadkhah, E. C. P. Neto, H. Mahdikhani, P. K. Danso, H. Molyneaux, and A. A. Ghorbani, "IoT Zigbee Device Security: A Comprehensive Review," *Internet of Things*, vol. 22, p. 100791, 2023, doi: 10.1016/j.iot.2023.100791.

[33] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT," *IEEE Access*, vol. 5, pp. 3302-3312, 2017, doi: 10.1109/ACCESS.2017.2684183.

[34] F. Ghorbani, A. Ahmadi, M. Kia, Q. Rahman, and M. Delrobaei, "A Decision-Aware Ambient Assisted Living System with IoT Embedded Device for In-Home Monitoring of Older Adults," *Sensors*, vol. 23, no. 5, p. 2673, 2023, doi: 10.3390/s23052673.

[35] J. Sangeetha and U. Kumaran, "A Hybrid Optimization Algorithm Using BiLSTM Structure for Sentiment Analysis," *Measurement: Sensors*, vol. 25, p. 100619, 2023, doi: 10.1016/j.measen.2023.100619.

[36] S. Mirjalili and A. Lewis, "The Whale Optimization Algorithm," *Advances in Engineering Software*, vol. 95, pp. 51-67, 2016, doi: 10.1016/j.advengsoft.2016.01.008.

[37] Li, Y., Meng, C., Tian, J., Fang, Z., & Cao, H. (2024). Data-Driven Customer Online Shopping Behavior Analysis and Personalized Marketing Strategy. Journal of Organizational and End User Computing (JOEUC), 36(1), 1-22.

[38] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, and I. Yaqoob, "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges," *IEEE Access*, vol. 5, pp. 5247-5261, 2017, doi: 10.1109/ACCESS.2017.2689040.

[37] Sayed, G. I., Darwish, A., & Hassanien, A. E. (2020). Binary whale optimization algorithm and binary moth flame optimization with clustering algorithms for clinical breast cancer diagnoses. Journal of Classification, 37(1), 66-96.

[38] Osman, Ismail Namiq, and Idress Mohammed Husien. "Comparison of Sentiment Analysis Techniques for Twitter posts classification." 2022 International Conference on Data Science and Intelligent Computing (ICDSIC). IEEE, 2022.

[39] Abdalrada, Ahmad, Ali Fahem Neamah, and Hayder Murad. "Predicting Diabetes Disease Occurrence Using Logistic Regression: An Early Detection Approach." Iraqi Journal For Computer Science and Mathematics 5.1 (2024): 160-167.

[40] Anwer, Zainab Alwan, Ahmad Shaker Abdalrada, and Ihtiram Raza Khan. "Assessing Institutional Performance Using Machine Learning Algorithms." Wasit Journal of Computer and Mathematics Science 3.3 (2024).