Inteligencia Artificial 27(74), 152-165
doi: 10.4114/intartif.vol27iss74pp152-165

INTELIGENCIA ARTIFICIAL

http://journal.iberamia.org/

DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments

Mehdi Ebady Manaa[1][2], Saba M. Hussain[2], Suad A. Alasadi[2], Hussein A.A.Al-Khamees [3]

[1] Intelligent Medical Systems Department, College of Sciences, Al-Mustaqbal University
[2] Department of Information Networks, College of Information Technology, University of Babylon
[3] Computer Techniques Engineering Department, College of Engineering and Technologies, Al-Mustaqbal University

Abstract In today's digital era, most electrical gadgets have become smart, and the great majority of them can connect to the internet. The Internet of Things (IoT) refers to a network comprised of interconnected items. Cloud-based IoT infrastructures are vulnerable to Distributed Denial of Service (DDoS) attacks. Despite the fact that these devices may be accessed from anywhere, they are vulnerable to assault and compromise. DDoS attacks pose a significant threat to network security and operational integrity. DDoS assault in which infected botnets of networks hit the victim's PC from several systems across the internet, is one of the most popular. In this paper, three prominent datasets: UNSW-NB 15, UNSW-2018 IoT Botnet and recent Edge IIoT are using in an Anomaly-based Intrusion Detection system(AIDS) to detect and mitigate DDoS attacks. AIDS employ machine learning methods and Deep Learning (DL) for attack mitigation. The suggested work employed different types of machine learning and Deep Learning (DL): Random Forest (RF), Support Vector Machine (SVM), Logistic Regression, and Multi-layer perceptron (MLP), deep Artificial Neural Network (ANN), and Long Term Short Memory (LSTM) methods to identify DDoS attacks. Both of these methods are contrasted by the fact that the database stores the trained signatures. As a results, RF shows a promising performance with 100% accuracy and a minimum false positive on testing both datasets UNSW-NB 15 and UNSW-2018 Botnet. In addition, the results for a realistic Edge IIoT dataset show a good performance in accuracy for RF 98.79% and for deep learning LSTM with 99.36% in minimum time compared with other results for multi-class detection.

Keywords: Internet of things (IoT), Cyber-security, Distributed denial of service (DDoS), Anomaly-based detection, RF classification algorithm.

1 Introduction

The Internet of Things (IoT) has grown to become the largest network in the world, with millions of devices communicating with one another to make human activities simpler and easier. This development has led to the IoT being dubbed" the fourth industrial revolution." According to the results of a recent poll, there had been 22 million sales of Amazon Echos and 310.4 million USD worth of sales of wearable gadgets by the end of 2017 [1]. Also, in preparation for the imminent explosion, it is projected that 30.73 billion Internet of Things devices will be installed by the year 2020, and %it is anticipated that this number will be more than quadruple in the space of only the following five this number is expected to more than quadruple within just the next five years [2].]. It needs a number of tasks to be completed at various levels over the whole IoT working period in order for any smart application to achieve its targeted result. There have been several reference models or frameworks of the Internet of Things (IoT) published in the literature with the purpose of better understanding how the IoT operates. Some of these models and frameworks are constructed of three levels, each of which represents one of three major functionalities in the fundamental model [3]. The perception layer, which is the first layer in the internet of things and the physical cornerstone of its ecosystem, concerns with the process of collecting data through the use of a

ISSN: 1137-3601 (print), 1988-3064 (on-line)

variety of sensing devices including, but not limited to sensors, RFID readers, smart controllers, and so on. The second layer, namely the network layer, takes the role of orchestrating the connection between the collected data and a verity of servers and devices to transmit and process the collected data smoothly [4]. The application layer is the third layer that delivers the processed information to a wide range of IoT applications from smart homes to the intelligent solutions of healthcare issues. These three layers in their holistic integration enable the IoT of uniting the physical realm and the digital one; revolutionizing the way of our perception, interaction and utilization of data in our world [5]. The application layer is where the action takes place. There are a range of smart applications that make use of the Internet of Things as a communication medium, including smart cities, smart homes, smart grids, and other similar applications [6].

The purpose of an attack known as a denial-of-service is to thwart the delivery of a service that is normally offered by an internet-connected application. This is achieved by causing unnecessary traffic, which results in the waste of network resources and the exhaustion of those resources [7]. DDoS assaults happen when a host server is bombarded with a huge number of pointless requests from a big number of zombie devices that are spread out in different parts of the world [8]. The majority of academics classify Internet of Things applications into four fundamental layers, with a few more auxiliary layers on top of that [9]. This is despite the fact that there is no standard architecture level for Internet of Things applications as of yet [10]. The application layer, the network layer, the middleware layer, and the perception layer make up the different components that make up the system. Every layer has flaws in its security that make it vulnerable to assault from a range of different attack vectors, including those that are outlined above [11].

This paper talks about the architecture of the Internet of Things as well as Protocols utilized at each tier, main problems and security concerns that make IoT vulnerable to assaults, major DoS/DDoS attacks that target distinct IoT levels, and viable responses and preventative strategies.

2 Related Works

This section presents an overview of several DDoS mitigation strategies within the context of IoT systems utilizing a fog computing network architecture. Several proposed systems with machine learning algorithms will be discussed in detail below.

The framework of [12] applied the logistic regression classifier to the CICDDoS-2019 dataset, and the results of the classifier were investigated using two different datasets. The first dataset includes an attack on Portmap, for which the binomial logistic regression method was used. The second dataset includes DDoS attacks on LDAP and NetBIOS, for which the multinomial logistic regression method was used to classify these two variants with normal data. Both datasets are examples of DDoS attacks. In the Portmap dataset, the accuracy was found to be 99.91 % percent with F1_score of 0.9913, while in the LDAP dataset, the accuracy was found to be 99.94 % with F1_score of 0.9847.

In [13], the author of presented a DDoS mitigation architecture for IoT that makes use of fog computing to enable rapid and accurate attack detection. A database and an anomaly-based approach of intrusion detection are utilized in the framework for mitigating risk. The k-NN classification technique is utilized by the anomaly-based detection system, which is responsible for identifying DDoS assaults. The database is used to record the signatures of previously discovered attacks. The k-NN classification method that suggested for this framework was evaluated using a DDoS-based dataset, and the results showed that it achieved an accuracy level that was sufficient in identifying DDoS assaults.

A new hybrid binary classification approach called DNN- KNN was proposed by the researchers of [14]. Because of its high accuracy and recall rates, it is an excellent candidate for use as the first level of the two-stage detection approach utilized by the described design. Deep Neural Networks (DNN) and an algorithm called K-Nearest Neighbor (KNN) form the foundation of this technique. It was analyzed using the publicly available NSL-KDD and CICIDS2017 datasets. The strategy of picking qualities depending on the pace of information gain was the one that we utilized. The methodology suggested in this work achieved an accuracy of 99.77% for the NSL-KDD dataset and 99.85 % for the CICIDS2017 dataset. The experiments demonstrated that the suggested hybrid technique obtained a higher level of precision than both traditional approaches to machine learning and the most current developments in intrusion detection for IoT devices. According to [15], a localized DDoS prevention architecture called FOGshield is proposed. It makes use of the federated computing capacity of fog computing-based access networks to deploy several smart endpoint defenders at the border of relevant attack-source/destination networks. A central orchestrator is in charge of monitoring the smart endpoint defenders' collaboration with one another. Based on the behavior of the attacker, the central orchestrator will locate each smart end-point defender by inputting the proper training parameters into the component of the self-organizing map that it controls. The performance of the FOGshield architecture is validated by utilizing three different scenarios that are representative of common IoT traffic.

Based on the study of [16], where the authors recommended making an adjustment to the design of GRU-RNN by utilizing SVM as the network's final output layer while per- forming a binary/non-probabilistic classification job. Because SVM has a faster prediction time compared to Softmax, this proposal was considered to have a good chance of passing. However, the validity and accuracy were recorded for the training and testing phases. The validity of the proposed model during training was 81.54%, and the accuracy of the model while testing was 84.15%. While, the accuracy of the latter model during training was 63.07%, and the accuracy during testing was 70.75%.

Since the Convolutional Neural Network (CNN) is an essential approach of deep learning techniques can use in the classification task [17], the implementation of CNN with a Bidirectional Gated Recurrent Unit (Bi-GRU) model for the purpose of intruder detection and classification has been described in reference [18]. The BiGRU model incorporated an attention method to discover the crucial aspects that contribute to the detection of DDoS attacks. Furthermore, the precision of the classification model is enhanced by the utilization of a nature-inspired meta-heuristic optimization technique known as the Wild Horse Optimization (WHO) algorithm. The system that has been provided demonstrated superior performance compared to the already available approaches in terms of accuracy 99.35 %, detection rate 98.99%, precision 99.9%, and F-Score 99.08% when applied to the APA DDoS attack dataset. Additionally, it achieved a high level of accuracy 99.71%, detection rate 99.02%, precision 99.89%, and F-score 99.05% when applied to the ToN-IoT dataset.

The authors of [19] utilized feature selection scheme that combines statistical test-based filter approaches, including Chi-Square (XX2), Pearson's Correlation Coefficient (PCC), and Mutual Information (MI), with a metaheuristic approach called Non-Dominated Sorting Genetic Algorithm (NSGA-II) for the purpose of optimizing features. The suggested approach utilized filter-based techniques to prioritize the features for guided population initialization in NSGA- II, resulting in expedited convergence towards a solution. The performance evaluation of the suggested method was conducted by utilizing the ToN-IoT dataset, with a focus on two key metrics; the number of chosen features and the accuracy achieved. The experimental results are contrasted with contemporary state-of-the-art approaches. The examination of the results revealed the exceptional performance of the suggested scheme, which used a minimal amount of optimized features (specifically, just 13 out of the total 43 characteristics). It achieved an accuracy as 99.48%.

In the reference [20], a robust solution is presented for detecting anomalies in IoT networks. This method applied a statistical approach to develop a DDoS attack detection system, incorporated three unique algorithms; EWMA, KNN, and CUSUM. The effectiveness of this model was evaluated using the Bot-IoT dataset. Based on the obtained findings, it can be inferred that this model was attained a considerable level of accuracy 99.0% while maintaining a minimal FPR. Many studies in cyberattacks detection for IoT paradigm have been proposed using various deep learning models, which aims to enhance attacks detection accuracy. The authors of [21] proposed a DeepAK-IoT model consisting of three main components: Residual, Temporal-based spatial representation (RSR/ TBS) blocks, and Detection block. Five residual blocks with parallel layers is used in RSR to mitigate vanish gradient issues. LSTM and GRU is TRB block is used to capture temporal data patterns for detecting cyber-attacks, and fully connected layer with Softmax activation for final classification. The results show good performance for three benchmark datasets TON-IoT, Edge-IIoT, and UNSW-NB15. The accuracy model was 90.5%, 94.96%, and 98.41% respectively.

According to [22], they conducted an evaluation and reviewing the effectiveness of IoT and IIoT cyberattacks collection to enhance the network security. The proposed method used the Edge-IIoT dataset in various machine learning methods. J48 and PART was achieved high accuracy in binary classification from 99.51 % to 99.55 % respectively. In multi-class scenario, the performance metric using accuracy face a challenges, which highlighting to use an advance technique to classify the cyberattack and handling the complexity of multi-class intrusion detection.

An intelligent system for IIoT cyberattacks using machine and deep learning is proposed by [23]. The implemented system used SVD for feature selection in the preprocessing step. SMOTE algorithm to solve the unbalance class distribution. Various machine learning (ML) and deep learning (DL) for class detection. The detection step used LSTM, BI-LSTM, GRU, decision trees and K-nearest neighbors for classification cyberattacks. The obtained results show that the accuracy was 99.99% for binary classification, and 99.9% for multi-class classification in average for all methods. This approach paves a way for a robustness IDS system against cyberattacks.

A deep learning for intrusion detection is proposed by [24], which combined two deep approaches CNN and GRU named AttackNet, to detect and classify cyberattacks with promised accuracy and efficiency. A testing accuracy was 99.75 % demonstrating a robustness model against various cyberattacks with high precision and recall score. This study proposes fog computing architecture for real- time DDoS detection and mitigation. Due to IoT devices, fog computing detects assaults quickly and accurately. Traffic randomness measurement and KNN method detect DDoS attacks. This system detects 100% TCP, 98.79% UDP, and 100% ICMP assaults.

3 Research Methodology

Internet of Things devices come with sensors that constantly send information about the environment and how the device itself is working. The Internet of Things is a place where all the data from these many devices can be stored in one place. The platform of the Internet of Things is made up of cloud servers and a huge amount of database storage. The IoT platform does the work on the data and mixes them together. Besides, the platform does a thorough investigation of data to pull out information that is important. Attackers can exploit security vulnerabilities in Internet of Things (IoT) devices, as demonstrated in the Mirai attacks of October 2016. In these attacks, a vast number of IoT devices were harnessed to launch a distributed denial-of-service (DDoS) attack, overwhelming internet networks with a barrage of requests. The platform will then send back instructions based on the information that was given as shown in figure 1.

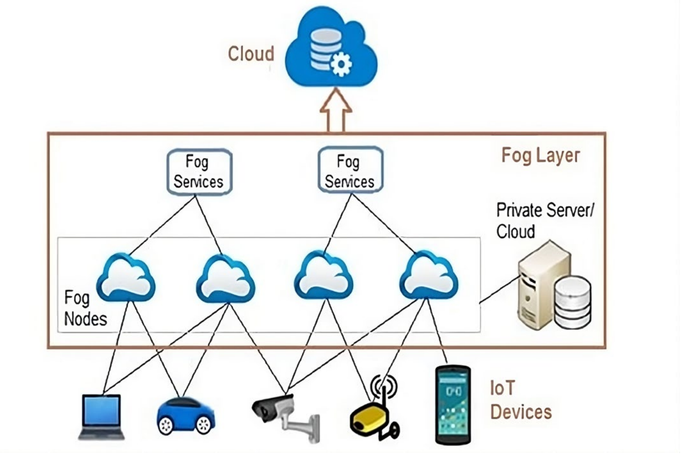

Figure 1. IoT platform work

Moreover, a visual representation is presented in figure 2 that depicts the proposed system's methodology. The procedural sequence commences with the crucial step of dataset ingestion. Subsequently, the dataset proceeds through a meticulous data pre-processing phase, where the values are subjected to modifications ensuring their suitability for analytical investigations. Data converting using entropy in equation (1) for 1 second are employed in three datasets.

$$H = -\sum_{i=0}^{n} P(x_i) log_2(x_i) \qquad (1)$$

Where, $H \geq 0$, and $0 \leq P(x_i) \leq 1$

Upon the successful conclusion of this preparatory phase, the processed dataset is strategically partitioned into two distinct segments. The first segment known as the training set, assumes the role of training a machine learning classifier. This phase involves exposing the classifier to patterns within the data, enabling it to discern the underlying relationships and features.

While, the second segment, referred to as the testing set, undertakes the pivotal task of evaluating the predictive capabilities of the trained classifier. Through this evaluation, the classifier's effectiveness in generalizing its learned insights to new, unseen data instances becomes apparent. As part of this examination, a comparison is drawn between the anticipated outputs based on the testing set and the actual outputs yielded by the classifier's predictions. This comprehensive approach elucidates how the proposed system orchestrates the progression from raw dataset to predictive modeling, encapsulating the key stages of data preparation, training, and assessment.

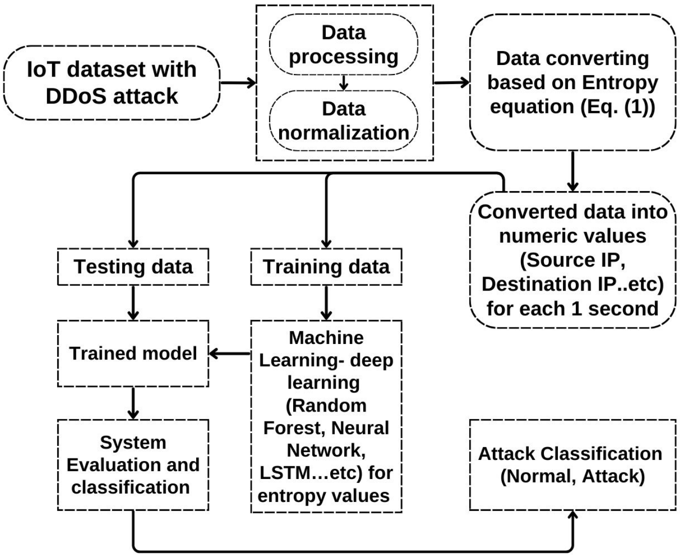
IoT dataset with DDoS attack
Data processing
Data normalization
Data converting based on Entropy equation (Eq. (1))
Converted data into numeric values (Source IP, Destination IP..etc) for each 1 second
Testing data
Training data
Trained model
Machine Learning- deep learning (Random Forest, Neural Network, LSTM...etc) for entropy values
System Evaluation and classification
Attack Classification (Normal, Attack)

Figure 2. The framework of the proposed system for DDoS attacks detection

4 Dataset and algorithm description

This section describes the datasets uses in the proposed system, then, the step of pre-processing to these datasets are discusses, and finally, an explanation of the machine learning techniques which are applies within the proposed system.

4.1 Dataset Description

In the current system, the researchers use three datasets that are; UNSW-NB 15, UNSW-2018-IoTBotnet and realistic collection of Edge IIoT datasets. However, these datasets contain a mixture of intrinsic modern normal operations and contemporary synthetic attack behaviors. In the investigation, only 78 dataset characteristics were UNSW-NB 15, and the best 10 dataset characteristics were UNSW-2018-IoTBotnet. Table 1 shows dataset parameters. Edge IIoT dataset will be described in more details in results section as a realistic cybersecurity collection.

Table 1: Comparison the UNSW-2018-IOT BOTNET and UNSW-NB15 datasets based on a variety of criteria

Parameter	UNSW-NB 15	UNSW-2018-IoT BOTNET
Year	2015	2018
Modern attacks	Yes	Yes
Feature selection	78	10
Publicly available	Yes	Yes
Label data	Yes	Yes

4.2 Data pre-processing

The proposed work performs on 225,747 data rows of UNSW-NB 15 and 291,320 of UNSW-2018-IoT Botnet. The next steps are conducted on the datasets as pre-processing step as in Eq. (2):

$$Z = \frac{x - \mu}{\sigma} \qquad (2)$$

where x is the future value. μ is mean and, σ is standard deviation.

1. Entropy calculation: It is planned to retrieve the data at regular intervals of one second until it has been properly investigated. While going through the process of packet analysis the entropy of the network has to

be measured in order to determine whether or not a DDOS attack has been launched against it. When the entropy is low, this would imply that all of the values are the same. On the other hand, when the entropy is high, it means that the random distribution is high. Based on the properties of the packet and the computation of the randomness, this concept might be utilized to identify the distributed denial of service attacks as shown in Eq. (1). The entropy of a group of packets is computed, with a value of 1 indicating a high degree of randomness and a value of 0 suggesting that all of the packets are the same as each other. This equation is used in three datasets for each (1) second in window time to extract entropy values. However, Eq. (1) describes the Entropy equation.

2. Standardization: The dataset is standardized before being used in the experiment normalization using a z-score method according to Eq. (2).

In the same context, the data is divided into: 70% as a training data and 30% as a testing data.

4.3 Machine Learning

In the proposed system, five machine learning (ML) classifiers are used as follows:

1) Logistic Regression (LR): A method of predictive analytics known as logistic regression is founded on the idea of probability. It is an algorithm of ma- chine learning used to solve classification issues. It is employed to classify observations into a variety of different categories instead of the most common linear function used in statistical analysis represented by LR method utilizes a more complicated cost function referred to as the "Sigmoid function" or simply the "logistic function", which is more sophisticated than the linear function. For the purpose of converting expected values to probabilities, the sigmoid function is used. Any value can convert into a value falls between 0 and 1 with this function. In machine learning, the mapping of predictions to probabilities is done with the help of the sigmoid function [25]. Eq. (3) indicates the general formula of sigmoid function:

$$f(x) = \frac{1}{1 + e^{-(x)}} \qquad (3)$$

2) Random Forest (RF): The random forest is a supervised approach of machine learning that can be used in tasks involving classification and regression. It is a method of categorization that organizes information by employing a large number of decision trees as the primary means of doing so. Each tree is built using bagging and randomization of its features to make a forest of trees whose predictions don’t match up with each other. The committee’s predictions are more accurate than those of any single tree [26]. One of the most essential characteristics of RF algorithm is its capacity to process datasets including both continuous and categorical variables, as is the case with regression and classification. When it comes to resolving categorization issues, it beats the rival products [27].

3) Multi-layer perceptron (MLP) is a feed-forward neural network (FFNN) that consists of one or more hidden layers, each containing one or more neurons [28]. This model extends the perceptron network, which is widely used in neural networks. A Multi-Layer Perceptron (MLP) that has only one hidden layer is referred to as a shallow neural network. By incorporating a sufficient number of hidden neurons, this type of network can accurately mimic almost any problem involving tabular data. By adding multiple hidden layers, the Multi-Layer Perceptron (MLP) is transformed into a deep neural network. Although adding additional hidden layers may provide slight advantages, it increases the computational expenses because of the significant increase in trainable parameters. This, in turn, worsens the likelihood of overfitting [29]. MLP consists of a solitary hidden layer, which has three levels of nodes: an input layer, a hidden layer, and an output layer. Information solely travels in a unidirectional manner, commencing with the input nodes, passing through the concealed nodes, and culminating at the output nodes. Every node, with the exception of the input nodes, acts as a neuron. It includes a bias neuron and performs calculations using a non-linear activation function [30].

4) Support Vector Machines (SVM): A wide variety of machine learning tasks can benefit from applying this technique, which is a kernel-based learning method- ology. The primary objective of SVMs is to solve a convex quadratic optimization problem in order to obtain a solution that is optimum on a global scale and so avoid the local extremum paradox; a difficulty that is encountered by other machine learning approaches. (SVM) offers a key advantages over many other statistical methods. In their basic form, SVMs function as linear binary classifiers, distinguishing between two classes based on a singular boundary. This ability to linearly segregate multidimensional data in the input space forms the foundation of the linear support vector machine (LSVM). By using training data as a guide, SVMs create an optimal hyperplane that divides the dataset into specific present classes [31]. SVM in its purest form, is a linear binary classifier, which means that it can only distinguish between two classes based on a single boundary. The notion that multidimensional data

in the input space may be linearly segregated is the foundation of the linear support vector machine (LSVM) [32].

5) To achieve the greatest possible separation or margin, SVMs use a subset of the training sample as support vectors. This subset is chosen based on its proximity in feature space to the ideal decision border. The training samples are the most challenging ones to be classified, and their positioning has a direct bearing on where the decision border ought to be placed. Analytical and geometrical methods can be used to define the ideal hyperplane, also known as the greatest margin [33]. It is a decision boundary that lowers the amount of mis-classification mistakes that occur during the training phase by first choosing a number of hyper-planes with no sample in between them and then, calculating the ideal hyperplane at the point where the margin of separation is the largest. The construction of a classifier that has an adequate decision boundary is an iterative process that is referred to as the learning process [34].

5 Results and discussion

Results show a good accuracy performance for UNSW-NB, UNSW-2018 IoT BOTNET and a realistic Edge IIoT cybersecurity collections in the following two sub-sections.

5.1 Results of Machine learning for UNSW-NB 15 and UNSW-2018 IoT BOTNET

The proposed work using entropy and machine learning for two datasets UNSW-NB15 and UNSW-2018 IoT BOTNET are evaluated using the accuracy metric and other metrics to detect and mitigate DDoS attacks. This study carries out on a computer equipped with an Intel Core i7 processor and 16 G.B of RAM. All four machine learning algorithms were evaluated using the UNSW-NB 15 dataset, involving 225,747 data fields, and the UNSW-2018- IoT Botnet dataset, which comprised 291,320 data fields. The proposed system evaluates using four different measurements that are; accuracy, precision, recall and, F1_score, that describe in Equations (4), (5), (6), and (7) respectively [35]:

$$Accuarcy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (4)$$

$$Precision = \frac{TP}{TP + FP} \qquad (5)$$

$$Recall = \frac{TP}{TP + FN} \qquad (6)$$

$$F1_{Score} = \frac{2 * TP}{2 * TP + FN + FP} \qquad (7)$$

Where: TP (True Positive), FP (False Positive), TN (True Negative), FN (False Negative). The performance of the proposed method is evaluating and comparing to choose the best algorithm as shown in figure 3 and figure 4.

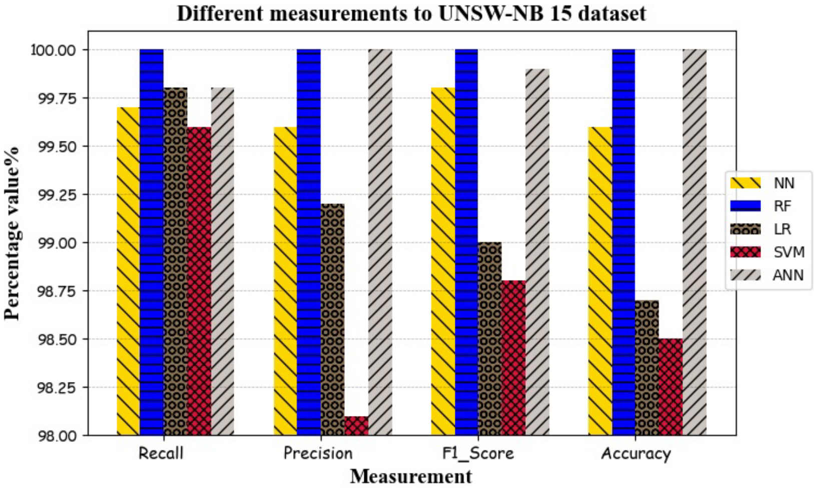

Figure 3. Evaluation of the proposed algorithms on UNSW-NB 15 dataset

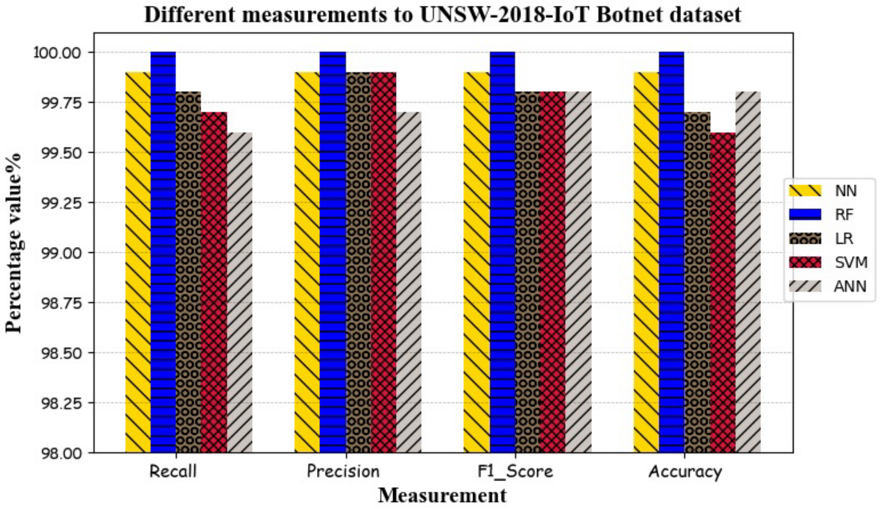

Figure 4. Evaluation of the proposed algorithms on UNSW-2018-IoT BOTNET dataset

It can be observed the superiority of the RF algorithm in term of accuracy of attack detection in comparison to the rest of the proposed algorithms for the UNSW-NB 15 and UNSW-2028 IoT datasets respectively.

Table II presents a summary of the confusion matrix of different classifier algorithms applied to both the UNSW- NB15 and UNSW-2018-IoT Botnet datasets. The confusion matrix is a fundamental tool in evaluating the performance of classification models. It offers valuable insights into the strengths and weaknesses of different classifier algorithms when tested on the two distinct datasets. The matrix's values enable a granular analysis of each algorithm's performance, helping researchers to better understand their behavior and make informed choices when selecting an algorithm for specific classification tasks. The different algorithms display varying levels of accuracy when tested on the two datasets.

Table II: Confusion matrix for classifiers

Dataset	Classifier	TP	TN	FN	FP
UNSW- NB 15	NN	28200	29343	61	119
	RF	38260	29461	1	1
	LR	38241	28705	20	757
	SVM	38127	28737	143	725
	ANN	38261	29457	5	0
UNSW-2018 IoT Botnet	NN	56306	912	35	47
	RF	56432	959	5	0
	LR	56306	901	131	58
	SVM	56248	903	189	56
	ANN	56316	922	25	37

It is clearly show that the table II highlights that the performance of each algorithm is influenced by the characteristics of the dataset it is applied to. For instance, this table shows that the (RF) algorithm achieves remarkably low false positives when tested on both datasets, indicating its proficiency in avoiding incorrect positive predictions. This is evident from the false positive count of 1 when applied to the UNSW-NB15 dataset and 0 when applied to the UNSW-2018-IoT Botnet dataset. In addition, (LR) algorithm demonstrates higher false negatives when tested on the UNSW-NB15 dataset compared to the UNSW-2018-IoT Botnet dataset. That is superior to all algorithms as well in terms of detection accuracy, as explained in Table III.

Table III: Comparison with other works

Reference	Year	Algorithm	ACC.
[36]	2020	RF	86.42 %
[37]	2019	DNN	99.19 %
[38]	2020	RF	94.8 %
Our method	2024	RF	100 %

5.2 Results of Machine learning and Deep Learning for Edge IIoT dataset

Furthermore, the proposed network architecture is implemented using the realistic collection of cyber security data for Internet of Things (IoT) and Industrial Internet of Things (IIoT). The dataset is created using IoT/IIoT testing environment, sensors, protocols, and cloud/ edge configurations [39]. The implemented work used entropy window for this real dataset each 1 second. The entropy considers the powerful toll for measuring the attack randomness. Table IV shows the main types of attacks before and after entropy for 1 second.

Table IV: Edge IIoT before and after windowing for 1 second

No.	Attack Type	No. of instances before entropy	No. of instances after entropy
1.	Backdoor-attack	24.862	5701
2.	DDoS-HTTP Flood-attack	229.022	252
3.	DDoS-ICMP Flood-attack	1.048.575	404
4.	DDoS-TCP-SYN Flood-attack	1.048.575	529
5.	DDoS-UDP Flood-attack	1.048.575	23018
6.	MITM-attack	1230	14
7.	Normal	24.301	16681
8.	OS-Fingerprinting attack	1.001	354
9.	Passward-attack	1.048.575	14915
10.	Port-Scanning attack	22.564	9973
11.	Ransomware -attack	10.925	4991
12.	SQL-injection attack	51.203	303
13.	Uploding-attack	37.634	137
14.	Valnerability scanner-attack	145.869	772
15.	XSS -attack	15.915	1667

It is clearly shown in the Table IV, the new entropy values dataset will be used in both the machine learning and deep learning. The main steps of implemented the entropy for each 1 second windowing as follows:

A. Cyberattacks files are collected from the website where it is free use of the Edge-IIoTset dataset for academic research purpose and public use as csv files.
B. All cyberattacks files were collected and combined into a single file after entropy windowing of 1 seconds.
C. The dominant class were label for each time window, where the class with high frequency is used to label each window entropy process.
D. Data shuffling is used for the previous step and save it in a new file as csv.

Then, the new saved file in the step (D) was used to fed the machine learning and deep learning to make a comparison with the other works. The machine learning algorithms were K-NN, RF, LR, and SVM. The implemented work proposed Edge IIoT attack classification model is based on K-NN, RF, LR and SVM to classify cyberattack data into 15 attacks plus the normal type. The accuracy evaluation metric shows that the details of the proposed system using machine learning on the Edge-IIoT realistic cybersecurity attacks data as follows; random forest has a high security of 98.79% and a time to build model of 11 ms, while MLP satisfied 98.73% with 5 ms time, SVM achieved 98.58 with 8 ms time. The lowest accuracy was conducted with logistic regression 86.79% and 11 ms time. Table V shows the main results of the machine learning by using 70% training and 30 % for testing for entropy values.

Table V: The results of machine learning for EDGE-IIoT 15 cyber-attacks classes

No.	Method Name	Accuracy	Time
1.	MLP Neural	98.73 %	5 ms
2.	Random Forest	**98.79 %**	11 ms
3.	Logistic Regression	86.5 %	8.2 ms
4.	SVM	98.58 %	8 ms

In the same context, Table VI explains the main Hyper-parameters that employed for each technique.

Table VI: The hyper-parameter values foe each technique

Technique	Parameter	Value
MLP	hidden layer sizes	100
	Max-iteration	200
	Activation type	Relu
	solver	Adam
SVM	kernel	Rbf
	C Regulation parameter	1.0
	gamma	Scale
Random Forest	Trees numbers in the forest	100
	Max-features	Auto
	Minimum number samples required to split at internal node	2
	Minimum number samples required to split at leaf node	1
LR	Fit-intercept	True
	Normalize	True

In addition, performance evaluation metrics in term of Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), and Error Rate (ER) are used in the proposed work for the machine learning methods. Table VII demonstrates the Edge-IIoT attacks detection of the evaluation metrics of the proposed algorithms, the Random Forest MAE as 0.02290 has lower the MAE value, which makes it superior compared with other methods. The results of MLP - MAE was 0.02413 in second level, while the SVM satisfied 0.02735 of MAE value.

Table VII: Different machine learning evaluation criteria for EDGE IIoT cyber-attacks

Evaluation Criteria	Machine Learning Technique			
	RF	SVM	LR	MLP
MAE	0.02290	0.02735	0.13275	0.02413
RMSE	0.23246	0.25394	0.46706	0.24114
ER	0.01167	0.01423	0.09750	0.01211

From Table VII, it is clearly shown that the minimum evaluation metrics of MAE value is achieved by Random Forest method as a 0.02290, while the lower value of RMSE is satisfies also by Random Forest method of 0.23246. Finally, the minimum of ER value is 0.09750 that done by LR method. Moreover, figure 5 demonstrates these evaluation metrics.

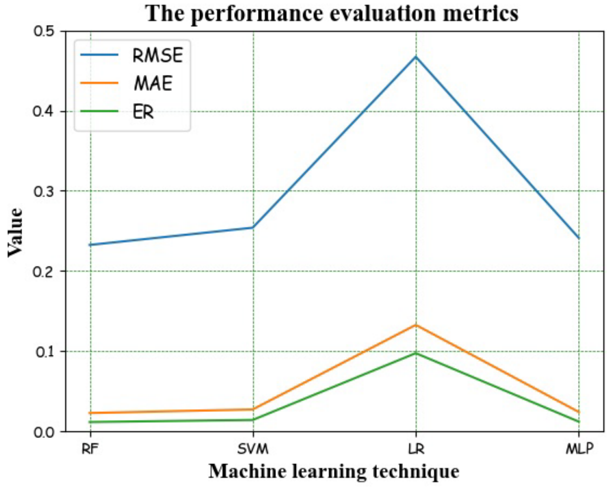

Figure 4. Evaluation metrics of different machine learning

The proposed work using the deep learning technique for both LSTM and ANN sequential model is implemented for Edge IIoT dataset. Table VIII shows the main Hyper-parameter used with deep learning.

Table VIII: Hyper-parameter for LSTM and ANN deep learning to EDGE IIoT dataset

Hyper-parameter	ANN deep learning	LSTM deep learning
Number of layers	5 with input layer	4 (3 LSTM + 1 Dense layer)
First layer neurons	128	128
Second layer neurons	64	64
Third layer neurons	32	32
Output layer neurons	15 with + normal class	15 with + normal class
Hidden layer activation function	Relu	NA
Output layer activation function	Softmax	Softmax
Optimizer	Adam	Adam
Type of loss Function	Categorical Cross-entropy	Categorical Cross-entropy
Batch Size	32	32
Number of Epochs	20	25

In the terms of accuracy metric, table IX expounds the accuracy metric for Edge-IIoT realistic cyber security data for 15 attacks asses. From this table, it can be observed that the ANN satisfied good accuracy for cybersecurity 15 attacks with minimum testing time. In the other hand, LSTM sequential deep learning takes more time with accuracy 99.36%.

Table IX: The accuracy metric for EDGE IIoT realistic cyber-security dataset

No.	Method Name	Accuracy	Training Time (ms)	Testing Time (ms)
1.	ANN	98.72 %	19391	257
2.	LSTM	99.36 %	9516	325

As a result, in experimental evaluations, we compare the proposed method with previous related methods that used the Edge-IIoT cyberattacks dataset that used 15 classes. Table X clarifies the results of these comparisons.

Table X: The main comparison between different approaches in the related works for 15 classes EDGE IIoT cyber-attacks dataset

Ref., Year	Dataset, Architecture	AI Technique	ACC. %
[21], 2023	Edge IIoT dataset multiclass	LSM and GRU	94.96
[22], 2023	Edge IIoT dataset multiclass	J48	92.92
[23], 2023	Edge IIoT dataset Multiclass only 10 classes with normal	SVD-GRU	99.9
		CNN and GRU	99.97
		MLP Neural	97.73
		RF	98.79
		LR	86.5
		SVM	98.58
[24], 2024	N-BaIoT dataset	ANN	98.72
[39], 2022	Edge IIoT dataset multiclass	Decision Tree (DT)	67.11
		RF	80.83
		SVM	77.61
		Deep Neural Network (DNN)	94.67
Our proposed method	Edge IIoT dataset multiclass	LSTM	**99.36**

6 Conclusion

The prevalence of modern technologies results in a rise in the number of internet-connected devices enabling significantly faster communication. As a result, safeguarding these devices, which can be controlled remotely, has become an essential need because attackers may take advantage of vulnerabilities to carry out extensive distributed denial of service attacks. The system's efficacy was rigorously evaluated using three distinct datasets: UNSW-NB15, UNSW-2018-IoT Botnet, and modern realistic Edge IIoT datasets. The results underscore its impressive accuracy in detecting and mitigating DDoS threats using machine learning techniques and deep learning with the entropy values. To comprehensively assess the proposed network's performance, sophisticated analysis is conducting on these datasets. The RF algorithm shows a superior in accuracy metric and less testing time, while the deep learning LSTM show a good accuracy with moderate time. This complete approach not only presents an innovative Random Forest (RF) and LSTM algorithm-based solution for mitigating DDoS threats but also, showcases its practical implementation through advanced implementation, establishing its potential to safeguard internet-connected devices in the contemporary digital landscape. In addition, this integration model for using entropy based window time show an effectiveness in detection an IoT attacks in real time.

Acknowledgements

The authors would like to express our deepest gratitude to the Al-Mustaqbal University and the College of Information Technology at the University of Babylon for their invaluable support in the publication of this paper.

References

[1] I. Hussain. Secure , Sustainable Smart Cities and the Internet of Things : Perspectives , Challenges , and Future Directions. *Sustainability*, 16(4):1390, 2024. doi: 10.3390/su16041390.

[2] G. P. Pinto, P. K. Donta, S. Dustdar, and C. Prazeres. A Systematic Review on Privacy-Aware IoT Personal Data Stores. *Sensors.* 24(7):1-23, 2024. doi:10.3390/ s24072197.

[3] A. Heidari, H. Shishehlou, M. Darbandi, N. Jafari, and N. Senay. A reliable method for data aggregation on the industrial internet of things using a hybrid optimization algorithm and density correlation degree. *Cluster Computing*. 4:1-19, 2024. doi: 10.1007/s10586-024-04351-4.

[4] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami. Internet of Things (IoT) Security Intelligence : A Comprehensive Overview , Machine Learning Solutions and Research Directions. *Mobile Networks Applications.* 28(1):296-312, 2022. doi: 10.20944/preprints202203.0087.v1.

[5] A. Hazra, P. Rana, M. Adhikari, and T. Amgoth. Fog computing for next-generation Internet of Things : Fundamental , state- of-the-art and research challenges. *Computer Science Review.* 48:100549, 2023. doi: 10.1016/j.cosrev.2023.100549.

[6] R. R. Nuiaa, S. Manickam, A. H. Alsaeedi, and E. S. Alomari. A new proactive feature selection model based on the enhanced optimization algorithms to detect DRDoS attacks. *International Journal of Electrical and Computer Engineering.* 12(2):1869-1880, 2022. doi: 10.11591/ijece.v12i2.pp1869-1880.

[7] A. N. Kadhim, and M. E. Manaa. Improving IoT data Security Using Compression and Lightweight Encryption Technique. In *Proc. of the 5th International Conference on Engineering Technology and its Applications (IICETA)*, pp. 187-192, 2022. doi: 10.1109/IICETA54559.2022.9888376.

[8] K. F. Hassan, and M. E. Manaa. Detecting distributed denial of service attacks in internet of things networks using machine learning in fog computing. In *Proc. of the 5th International Conference on Engineering Technology and its Applications (IICETA)*, pp. 323-328, 2022. doi: 10.1109/IICETA54559.2022.9888699.

[9] O. Ahmid, Maroua and Kazar, “A comprehensive review of the internet of things security,” *Journal of Applied Security Research.* 18(3):289-305, 2023. doi: 10.1080/19361610.2021.1962677.

[10] M. E. Manaa, and Z. G. Hadi. Scalable and robust cryptography approach using cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography.*23(7):1439-1445, 2020. doi: 10.1080/09720529.2020.1727609.

[11] V. V. Vegesna. Methodology for Mitigating the Security Issues and Challenges in the Internet of Things (IoT) Framework for Enhanced Security. *Asian Journal of Basic Science & Research.* 5(1):85-102, 2023. doi: 10.38177/AJBSR.2023.5110.

[12] M. J. Bhatta. Supervisor’s Recommendation. (Doctoral dissertation, TRIBHUVAN UNIVERSITY), 2019.

[13] M. A. Lawal, R. A. Shaikh, and S. R. Hassan. A DDoS attack mitigation framework for IoT networks using fog computing. *Procedia Computer Science.* 182:13-20, 2021. doi: 10.1016/j.procs.2021.02.003.

[14] C. A. D. Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. d. S. Vieira. Hybrid approach to intrusion detection in fog-based IoT environments. *Computer Networks.* 180:107417, 2020. doi: 10.1016/j.comnet.2020.107417.

[15] N. N. Dao, T. V. Phan, U. Sa’ad, J. Kim, T. Bauschert, and S. Cho. Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning. *IEEE System Journal.* 16(2):1974-1983, 2021. doi: 10.1109/JSYST.2021.3084199.

[16] T. Radivilova, L. Kirichenko, D. Ageiev, and V. Bulakh. Classification Methods of Machine Learning to Detect DDoS Attacks. In *Proc. of the 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pp. 207–210, 2019. doi: 10.1109/IDAACS.2019.8924406.

[17] H. A. A. Al-Khamees, W. R. H. Al-jwaid, and E. S. Al-shamery, “The Impact of Using Convolutional Neural Networks in COVID-19 Tasks : A Survey. *International Journal of Computing and Digital Systems*. 11(1):189-197, 2022. doi: 10.12785/ijcds/110194.

[18] K. Kethineni, and G. Pradeepini. Intrusion detection in internet of things-based smart farming using hybrid deep learning framework. *Cluster Computing.* 27(2):1719-1732, 2024. doi: 10.1007/s10586-023-04052-4.

[19] A. K. Dey, G. P. Gupta, and S. P. Sahu. Hybrid Meta-Heuristic based Feature Selection Mechanism for Cyber-Attack Detection in IoT-enabled Networks. *Procedia Computer Science.* 218: 318–327, 2023. doi: 10.1016/j.procs.2023.01.014.

[20] R. J. Alzahrani, and A. Alzahrani. A Novel Multi Algorithm Approach to Identify Network Anomalies in the IoT Using Fog Computing and a Model to Distinguish between IoT and Non-IoT Devices. *Journal of Sensor and Actuator Networks.* 12(2):1-19, 2023. doi: 10.3390/jsan12020019.

[21] W. Ding, M. Abdel-Basset, and R. Mohamed. DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks. *Information Science.* 634:157-171, 2023. doi: 10.1016/j.ins.2023.03.052

[22] T. Al Nuaimi , S. Al Zaabi , M. Alyilieli , M. AlMaskari , S. Alblooshi , F. Alhabsi , M. F. Bin Yusof , and A. Al Badawi. A comparative evaluation of intrusion detection systems on the edge-IIoT-2022 dataset. *Intelligent System with Applications.* 20:200298, 2023. doi: 10.1016/j.iswa.2023.200298.

[23] S. Soliman, W. Oudah, and A. Aljuhani. Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal.* 81:371–383, 2023. doi: 10.1016/j.aej.2023.09.023.

[24] H. Nandanwar, and R. Katarya. Deep learning enabled intrusion detection system for Industrial IOT environment. *Expert Systems with Applications.* 249:123808, 2024. doi: 10.1016/j.eswa.2024.123808.

[25] K. F. Hassan, and M. E. Manaa. Detection and mitigation of DDoS attacks in internet of things using a fog computing hybrid approach. *Bulletin of Electrical Engineering and Informatics.* 11(3):1604–1613, 2022. doi: 10.11591/eei.v11i3.3643.

[26] J. J. M. Lamas, and L. R. W. Portillo. Web architecture for URL-based phishing detection based on Random Forest , Classification Trees , and Support Vector Machine. *Inteligencia Artificial.* 25(69):107–121, 2022. doi: 10.4114/intartif.vol25iss69pp107-121.

[27] A. Villa-murillo, A. Carrion, and A. Sozzi. Forest-Genetic method to optimize parameter design of multiresponse experiment, *Inteligencia Artificial.* 23(66):9–25, 2020. doi: 10.4114/intartif.vol23iss66pp9-25.

[28] H. A. A. Al-Khamees, N. Al-A'araji, and E. S. Al-Shamery. Classifying the Human Activities of Sensor Data Using Deep Neural. In *Proc. of the International Conference on Intelligent Systems and Pattern Recognition*. pp. 107-118, 2022. doi: 10.1007/978-3-031-08277-1_9.

[29] Y. Amethiya, P. Pipariya, S. Patel, and M. Shah. Comparative analysis of breast cancer detection using machine learning and biosensors. *Intelligent Medicine.* 2(2):69–81, 2022. doi: 10.1016/j.imed.2021.08.004.

[30] A. Al Bataineh, and S. Manacek. MLP-PSO Hybrid Algorithm for Heart Disease Prediction. *Journal of Personalized Medicine.* 12(8):1208, 2022, doi: 10.3390/jpm12081208.

[31] S. M. Elsedimy, H. Elhadidy, and S. M. M. Abohashish. A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer. *Cluster Computing.* 8:1-19, 2024, doi: 10.1007/s10586-024-04458-8.

[32] G. K. Kumar, M. L. Bangare, P. M. Bangare, C. R. Kumar, R. Raj, J. L. Arias‑Gonzáles, B. Omarov, and MD. Solaiman Mia. Internet of things sensors and support vector machine integrated intelligent irrigation system for agriculture industry. *Discover Sustainability.* 5(1):6, 2024. doi: 10.1007/s43621-024-00179-5.

[33] M. Jeyaselvi, M. Sathya, S. Suchitra, S. J. A. Ibrahim, and N. S. K. Chakravarthy. SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks. In *Proc. of Advances in Information Communication Technology and Computing (AICTC)*. pp. 461–471, 2022. doi: 10.1007/978-981-19-0619-0_41.

[34] H. A. A. Al-Khamees, N. Al-A'araji, and E. S. Al-Shamery. An Evolving Fuzzy Model to Determine an Optimal Number of Data Stream. *International Journal of Fuzzy Logic and Intelligent Systems.* 22(3):267-275, 2022. doi: 10.5391/IJFIS.2022.22.3.267.

[35] A. Flores, H. Tito-Chura. and L. Zea-Rospigliosi. Prediction of Research Project Execution using Data Augmentation and Deep Learning. *Inteligencia Artificial.* 26(71):46-58, 2023. doi: 10.4114/intartif.vol26iss71pp46-58.

[36] M. A. Umar, C. Zhanfang, and Y. Lui. Network Intrusion Detection Using Wrapper-based Decision Tree for Feature Selection. In *Proc. of the 2020 International Conference on Internet Computing for Science and Engineering.* pp. 5-13, 2020. doi: 10.1145/3424311.3424330.

[37] O. Faker and E. Dogdu. Intrusion Detection Using Big Data and Deep Learning Techniques. In *Proc. of the 2019 ACM Southeast conference*. pp. 86-93, 2019. doi: 10.1145/3299815.3314439.

[38] A. Golrang, A. M. Golrang, S. Y. Yayilgan, and O. Elezaj. A Novel Hybrid IDS Based on Modified NSGAII-ANN and Random Forest. *electronics.* 9(4):577, 2020. doi: 10.3390/electronics9040577.

[39] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, Land H. Janicke. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access*. 10:40281-40306, 2022. doi: 10.1109/ACCESS.2022.3165809.