Journal of
Sensor and Actuator Networks

MDPI

Article

Refined LSTM Based Intrusion Detection for Denial-of-Service Attack in Internet of Things

Kuburat Oyeranti Adefemi Alimi [1,*], Khmaies Ouahada [1], Adnan M. Abu-Mahfouz [1,2], Suvendi Rimer [1] and Oyeniyi Akeem Alimi [1]

[1] Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa; kouahada@uj.ac.za (K.O.); a.abumahfouz@ieee.org (A.M.A.-M.); suvendir@uj.ac.za (S.R.); oalimi@uj.ac.za (O.A.A.)
[2] Council for Scientific and Industrial Research, Pretoria 0001, South Africa
* Correspondence: kadefemi@uj.ac.za

Abstract: The Internet of Things (IoT) is a promising technology that allows numerous devices to be connected for ease of communication. The heterogeneity and ubiquity of the various connected devices, openness to devices in the network, and, importantly, the increasing number of connected smart objects (or devices) have exposed the IoT network to various security challenges and vulnerabilities which include manipulative data injection and cyberattacks such as a denial of service (DoS) attack. Any form of intrusive data injection or attacks on the IoT networks can create devastating consequences on the individual connected device or the entire network. Hence, there is a crucial need to employ modern security measures that can protect the network from various forms of attacks and other security challenges. Intrusion detection systems (IDS) and intrusion prevention systems have been identified globally as viable security solutions. Several traditional machine learning methods have been deployed as IoT IDS. However, the methods have been heavily criticized for poor performances in handling voluminous datasets, as they rely on domain expertise for feature extraction among other reasons. Thus, there is a need to devise better IDS models that can handle the IoT voluminous datasets efficiently, cater to feature extraction, and perform reasonably well in terms of overall performance. In this paper, an IDS based on redefined long short-term memory deep learning approach is proposed for detecting DoS attacks in IoT networks. The model was tested on benchmark datasets; CICIDS-2017 and NSL-KDS datasets. Three pre-processing procedures, which include encoding, dimensionality reduction, and normalization were deployed for the datasets. Using key classification metrics, experimental results obtained show that the proposed model can effectively detect DoS attacks in IoT networks as it performs better compared to other methods including models from related works.

Keywords: attacks; CICIDS-2017; deep learning; denial of service; intrusion detection system; internet of things; long short-term memory; machine learning; multilayer perceptron; NSL-KDS; refined long short-term memory

check for updates

Citation: Adefemi Alimi, K.O.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S.; Alimi, O.A. Refined LSTM Based Intrusion Detection for Denial-of-Service Attack in Internet of Things. *J. Sens. Actuator Netw.* **2022**, *11*, 32. https://doi.org/10.3390/jsan11030032

Academic Editor: Ugo Fiore

Received: 29 April 2022
Accepted: 2 June 2022
Published: 1 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In recent years, IoT has been adjudged as one of the most innovative technologies in computing, as it has the potential of changing every sphere of human life [1]. According to [2–6], by 2020 to 2025, it is expected that the number of smart devices connected to the Internet will reach up to 50 billion and 75 billion, making it one of the fastest-growing areas in the history of computing. IoT aims to connect devices and enables machine-to-machine communication, thereby allowing devices to exchange information without human involvement [7]. IoT covers a large variety of applications such as smart homes, smart cities, smart metering, agriculture, smart grids, smart healthcare, etc. [8,9]. Due to the increasing advancements in information and communication technology, and the global cybersecurity

issues, security and privacy concerns have been generally identified as a major challenge of IoT deployment. The extensive deployment of IoT devices in an open environment has exposed the networks to various cyberattacks and security threats [10]. Numerous cyberattacks such as replay, wormhole, Sybil, man-in-the-middle (MITM), denial of service (DoS), side-channel, etc., have continued to be a menace [11–13]. Hence, it is important to develop an effective security measure that can constantly and urgently learn and detect attacks such as DoS attacks in IoT networks.

Signature-based and anomaly-based intrusion detection systems (IDS) have been identified as security solutions for mitigating attacks and intrusions into IoT networks. Numerous IDS techniques have been proposed in the literature, using varieties of methods including mathematical formulations, data mining such as machine learning approaches, etc. [14–16]. These statistical formulations and the traditional machine learning models struggle in handling the high-dimensional IoT data, thus leading to poor performances. Hence, better methodologies, such as deep learning approaches hold great importance.

Deep learning has been extensively proposed for IDS in recent years due to its strong learning and feature extraction capabilities, especially in situations involving voluminous datasets. Deep learning techniques use multiple layers to gradually extract significant features from the raw input without domain expertise [17,18]. In this paper, we propose a refined long short-term memory (RLSTM), an advanced recurrent neural network (RNN) deep learning model for DoS attack detection in IoT. Due to the limited availability of real-time IoT network traffic datasets, researchers make use of simulated datasets as well as publicly available datasets which show real-life attributes of network traffic and recent attack scenarios. Two publicly available datasets with network traffic similar to real-life IoT network traffic; NSL-KDD and CICIDS-2017 datasets were used to test the effectiveness of the developed RLSTM model. Three preprocessing steps were deployed on the datasets and the results were compared to other methods including models from related works. The main contributions of the paper are summarized below:

- We present an effective model based on an improved deep learning algorithm for detecting and classifying intrusions in IoT.
- We proposed a refined long short-term memory (RLSTM) model which can detect denial-of-service (DoS) intrusions with a high level of accuracy using two voluminous traffic datasets, namely, NSL-KDD and CICIDS-2017 datasets to test the performance of the proposed model.
- To boost the classification performance of the developed model, we performed encoding, dimensionality reduction, and normalization preprocessing procedures on the two datasets.
- We deployed the following performance evaluation metrics: precision, recall, F1-score, and classification accuracy to assess the effectiveness of the proposed models.
- For evaluation, we compared the performance of the modeled RLSTM model with other machine learning methods using both NSL-KDD and CICIDS-2017 datasets. The experimental results illustrate that the modeled RLSTM model is very suitable for IoT intrusion detection. The performance of the RLSTM model is superior to the other considered classification methods on the two datasets.

The rest of the paper is structured as follows. Section 2 presents related works. Section 3 presents the proposed IDS model. Section 4 presents the experimental evaluation. Section 5 presents the results and discussions. Section 6 presents the threat to validity while Section 7 presents the conclusions.

Overview of Denial-of-Service (DoS) Attack

A denial of service (DoS) attack can be described as an attempt by malicious attackers to consume network resources or bandwidth by temporarily or indefinitely disrupting the network services of a computer or any devices connected to a network [12]. They are the most common and dangerous cyberattack against IoT devices which leads IoT systems to total shut down [19]. According to Hussain et al., DoS and DDoS attacks are increasing

in frequency and intensity, with an average of 28.7 K attacks per day [20]. Due to the low computational power and battery power of IoT devices, DoS attack on an IoT network has the potential to be more damaging [21]. Mahmoud et al. also explained that the network layer of IoT is mostly susceptible to DoS attacks [22]. The heterogeneity of the various connected devices and most importantly, the increasing number of connected smart devices has exposed the IoT to various DoS attacks. These attacks are currently preventing IoT from reaching its full potential. For instance, a massive DoS attack scenario within the IoT networks was performed against the anti-spam organization Spamhaus in March 2013 [23].

DoS attacks can be categorized into two: those that crash services and those that flood services. Distributed denial of service (DDoS) attacks are the most serious attacks [24]. The DDoS attack has caused significant damage to the IoT ecosystem. As a result, IoT users paid close attention to the threats. In 2016, the attacks continued to have an impact on IoT devices, which had the highest record in terms of cyberattacks in 2016 [25]. According to Akamai researchers, IoT devices account for roughly 21% of all DDoS attacks worldwide [26]. The DDoS attack is a type of DoS attack whereby multiple systems or machines or devices operate together to carry out an attack on a single target, which makes it difficult to track and turn off the attack machines. DDoS attackers often use a botnet to disrupt network services [27,28]. On 21 October 2016, the biggest DDoS attack was performed using Mirai IoT malware. The consequences of this attack were hours-long outages and service interruptions for some popular websites such as Amazon, Netflix, Twitter, and others [29,30]. According to Balaban, in 2014, a DDoS attack estimated at 400 gigabits per second slammed Cloudflare, a cybersecurity service and content delivery network [31]. Similarly, on 28 February 2018, GitHub, a software development platform, was subjected to a DDoS attack that clocked in at 1.35 terabits per second [31]. Various attacks instigated by DoS and DDoS attackers in the IoT environment include the Slowloris attack, UDP flood attack, ping flood attack, HTTP flood attack, jamming attack, wormhole attack, smurf attack, Mirai botnet, SYN flood attack, etc. Although different approaches to the mitigation of DoS and DDoS attacks have been proposed, the main defense mechanisms can be divided into three categories: prevention, detection, and mitigation.

2. Related Works

Intrusion detection systems (IDSs) are prominent security systems that are widely used for detecting and mitigating intrusions in IoT and other similar networks. However, the existing traditional IDSs that are based on statistical formulations are mostly inefficient and insufficient for the rapid mitigation of IoT intrusions. The use of data mining techniques such as machine learning and deep learning for intrusion detection in IoT is rapidly growing as they offer effectiveness and are computationally inexpensive. Various data mining models have been proposed in the literature for IoT network IDS in recent times. Verma et al. proposed an anomaly-based IDS for DoS attacks detection in IoT networks. The authors proposed different shallow machine learning algorithms including random forest (RF), Adaboost (AB), GBM, ERT, CART, and multi-layer perceptron neural network (MLP) for analyzing samples from CIDDS-001, UNSWNB15, and NSL-KDD datasets. From the experimentation, the authors achieved the best results from RF with an accuracy of 94% [32]. Similarly, Mohammed et al. compared the results of Nave Bayes, Bayes Net, and ZeroR machine learning algorithms for the detection and classification of attacks in IoT devices. The UNSW-NB15 dataset samples were utilized to assess the models' performance [33]. Likewise, Chopra et al. presented a comparative analysis of several shallow machine learning algorithms, which include Naïve Bayes, J48, RF, and ZeroR machine learning classifiers to detect and classify DDos attacks in IoT. The BoT-IoT dataset was used to evaluate the performance of the models [34]. An IDS using MLP for detecting DoS attacks in IoT networks was proposed by Hodo et al. The proposed method effectively detected various types of DDoS and DoS attacks with high accuracy [35]. Additionally, Mohammed et al. proposed an IDS based on multiple machine learning algorithms which include DT, k-NN, and NB for detecting DDoS attacks on IoT devices. The authors eval-

uated their experiments on CICIDS-2019 dataset samples and achieved an accuracy of 100%, 98%, and 29% from the three algorithms, respectively. However, as shallow machine learning algorithms often perform poorly especially with low accuracy when deployed on a huge amount of training data, the various described models may not perform well when deployed on voluminous IoT datasets [36]. Cvitić et al. proposed a DDoS traffic detection model that uses a boosting method of logistic model trees for different IoT device classes. From the experimentation, the authors achieved 99.92% to 99.99% accuracy for the four device classes. Their work takes classes of IoT devices into consideration [37]. Roopak et al. proposed an IDS based on a convolutional neural network (CNN), integrating long short-term memory (LSTM) deep learning techniques for classifying DDoS attacks. The experiment was evaluated on CISIDS-2017 datasets, which achieved an accuracy of 99.03%, precision of 99.26%, recall of 99.35, and an F1-score of 99.36% [38].

As alternatives, Susilo et al. proposed an IDS for detecting DoS attacks using RF, MLP, and convolutional neural networks (CNN). Using the BoT-IoT dataset for experimentation, the authors acknowledged the deep learning algorithm: CNN as the best performer with an accuracy of 91.27% compared to the 79.01% achieved by the MLP [39]. Ma et al. also presented a CNN deep learning-based detection model for detecting DDoS attacks in IoT using NSL-KDD datasets for evaluation. The authors were able to attain a 92.99% accuracy rate [40]. IoT attack detection mechanisms based on CNN and LSTM to detect DDoS attacks in IoT were proposed by Sahu et al. The authors evaluated the developed model using the dataset from the Stratosphere lab published in 2020 and they achieved an accuracy of 96% for the simulated attack detection [41]. In addition, Roy et al. proposed a bi-directional LSTM deep learning technique for IDS in IoT. The paper focuses on the binary classification of normal and attack patterns on the IoT network. The proposed model is trained using samples from the UNSWNB15 dataset, and the experimental results achieve a 95% accuracy rate in attack detection. However, the model is only trained using 5451 test samples from a single dataset. Aside from that, it provides no comparison to other recent models [42].

We sought to improve the shortcomings in the above-mentioned literature, such as scalability, efficiency, and effectiveness in the mitigation of intrusions involving voluminous IoT datasets. In addition, we sought to provide a viable security mechanism to address one of the most significant modern-day attacks with recently generated datasets that embodies the qualitative and quantitative characteristics of modern-day IoT traffic. Therefore, inspired by the broad acceptance of LSTM as a powerful recurrent neural network variant, with the capability to learn order dependence in sequence classification problems, an attempt has been made in this work to implement a refined LSTM intrusion detection model for detecting DoS attacks in an IoT.

3. Proposed IDS Model

This section presents the description of the proposed method with a detailed step-by-step process.

3.1. Refined Long Short-Term Memory (RLSTM)

RLSTM is a type of recurrent neural network (RNN) proposed by Sepp Hochreiter and Jürgen Schmidhuber in 1997 [43]. RLSTMs are highly rated RNN variants as they have the capability to tackle the problem of long-term dependencies of RNN [44]. In addition, they provide long-term memory, and they have the capacity of addressing the problem of vanishing gradients that might occur when training traditional RNNs [45,46]. They can process an entire sequence of data and not just the single data points. RLSTM prevents backpropagated errors from exploding. Instead, errors can flow backward via an infinite number of virtual layers that have been unfolded in space. Unlike the typical RNN whereby, their efficiency reduces as the gap length increases, RLSTM has an advantage of relative insensitivity to gap length. RLSTM network components include a cell, an input gate, an output gate and a forget gate. The cell is responsible for remembering the values at an exact time and the three gates control how information enters and leaves the cell [44]. The three

gates are briefly described: (1) Forget gate: this gate decides whether to keep information from the previous hidden state and the current input or delete it. This information is passed through the sigmoid function and the results are between 0 and 1. The value that is closer to 0 indicates forget while the value that is closer to 1 indicates keep. (2) Input gate: the input gate determines which information will be stored in the cell state. Information is updated using a sigmoid and tanh function. The sigmoid and tanh function decides which part of the information needs to be updated. Finally, the output value generated from these functions is used to update the cell state. (3) Output Gate: this gate decides the final output by employing a sigmoid function to select useful information from the current cell state as the output while the tanh function obtains the final output. Mathematically, the RLSTM gates can be expressed as [47,48]:

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

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (2)$$

$$c_t = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \quad (3)$$

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad (4)$$

$$h_t = o_t \cdot \tanh(c_t) \quad (5)$$

where f_t is the forget gate, σ is the sigmoid function, W_f is the weight between forget and input gate, h_{t-1} is the previous hidden state, x_t is the input at the current timestamp, i_t is the input gate at time t, W_i is the weight of the respective gate, tanh is the tangent function, W_c is the weight of tanh operator between cell state and network output and b_c is the bias wrt to W_c, o_t denotes the output gate at time t, W_o is the weight of output gate, b_f, b_i, b_o are the bias, h_t is the LSTM output, and c_t is the cell state.

3.2. RLSTM Experimental Setup

The proposed model was conducted using MATLAB on an Intel Core i5 CPU with 8 GB RAM. The experimental setup comprises (1) pre-processing step, (2) the RLSTM model training process, and (3) the testing and evaluation step, which is summarized in the flowchart depicted in Figure 1. Data preprocessing was prioritized, (i.e., 1-to-N encoding, normalization, dimensionality reduction); thus, we deployed these steps to prepare the data before training the model. Afterward, each pre-processed dataset is partitioned into training and testing sets, respectively. The pre-processed data are fed into the RLSTM components individually which extract the accurate feature representation of the data, respectively. We build an RLSTM model composed of an input layer with 25 and 65 features, and a hidden layer with 100 and 120 neurons for the two datasets, respectively. To achieve the best results, we employed a grid search approach to select the learning rate. The learning rate used was 0.01 and 0.001 on 150 and 100 batch sizes, respectively. The training reaches the minimum value of 50 and 13 epochs for the two datasets, respectively. The adaptive moment estimation (Adam) optimizer is deployed to update the weight of the RLSTM network. The SoftMax activation function was used to classify the learned features and identifies the intrusion behaviors as normal or abnormal. To enhance efficiency, cross-entropy is utilized as the loss function. Table 1 depicts the training parameters used in the model implementation. These parameters were chosen because they resulted in the optimal outcomes from several initial trials. The pseudocode of the RLSTM model is shown in Algorithm 1.

Algorithm 1: RLSTM Model

1	**Load Datasets**	Datasets: NSL-KDD; CICIDS-2017 (training sets and testing sets);
2	**for**	Data in Training and Test datasets **do**
3		Extract Features (x)
4		Extract Labels (y)
	Input:	Features Extracted from Datasets
	Output:	Classification results
5	**for**	Features in x **do**
		if datasets feature = non-numerical **then**
		Encode using 1-to-N encoding
6	**Normalize features**	Using Min-max normalization $x' = \frac{x-\min(x)}{\max(x)-\min(x)}$
7	**Training**	Train RLSTM model using the NSL-KDD and CICIDS-2017 training set;
		Add activation function = Softmax;
		Then classify;
8	**Testing**	RLSTM model testing
		Testing sets are fed into the RLSTM to detect attacks;
9	**Evaluation:**	
		Compute (loss = 'cross entropy', optimizer = 'adam')
		Compute classification results using {accuracy, precision, recall and f1-score}
10	**Output:**	Classification results

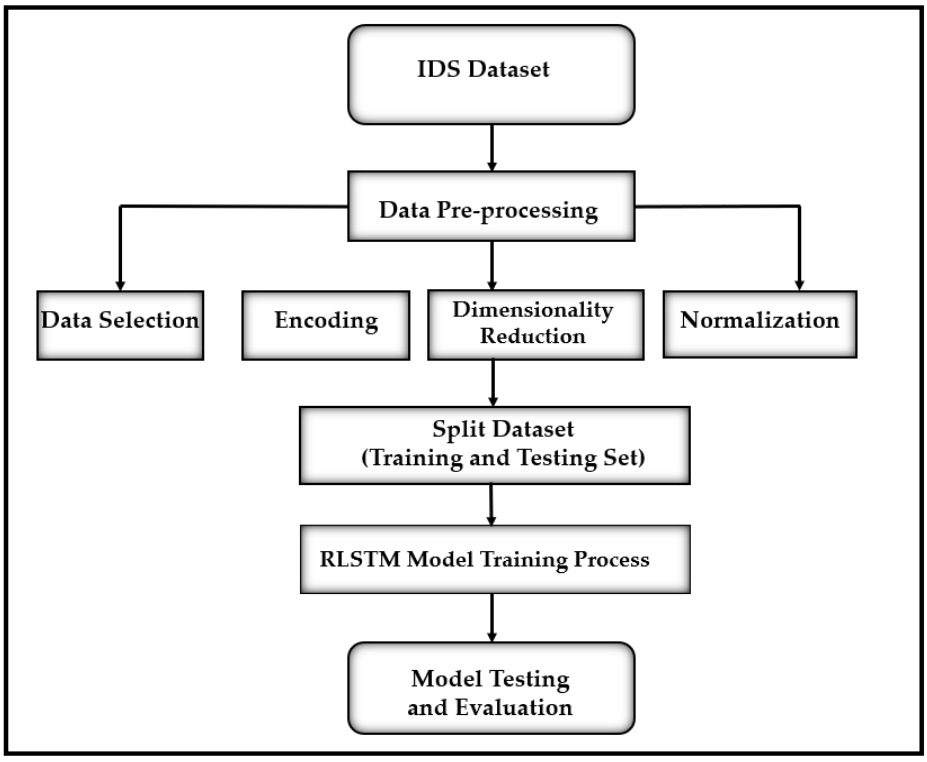

Figure 1. The proposed RLSTM flowchart.

Table 1. RLSTM parameters.

Parameter	NSL-KDD Specification	CICIDS-2017 Specification
Sequence input layer	1	1
Sequence input length	25 features	65 features
Number of hidden layers neurons	100	120
Number of fully connected layers	2	2
Activation function	Softmax	Softmax
Optimizer	Adam	Adam
Batch size	150	100
Epochs	50	13
Learning rate	0.01	0.001

4. Experimental Evaluation

The following sub-sections describe the dataset used in the study, the pre-processing steps, and the evaluation step.

4.1. Used Datasets

The datasets employed in this experiment are the NSL-KDD and CICIDS-2017 datasets.

The NSL-KDD dataset was developed by Tavallaee et al. in 2009 [49] to improve some of the shortcomings of the KDD99 dataset, which is the most deployed intrusion detection dataset but contains a huge number of duplicate and redundant records [49]. The NSL-KDD dataset is one of the currently available public datasets that provide labels for both training and testing sets, which comprise 24 and 38 attack types, respectively. The dataset contains simulated attacks made up of network traffic. For our experiment, we utilize the NSL-KDD dataset because it does not contain a huge number of redundant records. Additionally, the amount of repetitive data is minimized in the dataset. This dataset consists of 125,973 network flow data, 41 features, and 1 class attribute, which is marked as normal or attack. The NSL-KDD dataset comprises denial of service (DoS), user to root (U2R), remote to local (R2L), and probing attacks. In this study, DoS attacks were analyzed. Table 2 gives the summary of this dataset.

Table 2. Summary of NSL-KDD dataset.

Traffic	Normal	U2R Attack	DoS Attack	R2L Attack	Probing Attack
Training	67,343	52	45,927	995	11,656
Testing	9711	200	7458	2887	2421

The CICIDS-2017 dataset is a recently generated open-source dataset provided by the Canadian Institute of Cybersecurity for intrusion detection. The CICIDS-2017 dataset has the attributes of practical real-life network traffic, and its labeling is based on the timestamp, source and destination IPs, source and destination ports, protocols, and attacks [50]. This dataset was captured over a duration of 5 days with 2,830,743 records, 80 network traffic features, and 15 attack types. The dataset is the collection of real-world data which comprises eight traffic monitoring sessions in the form of a CSV file that contains normal and intrusion traffic. The normal traffic is described as 'benign' while the latter is referred to as 'attacks'. From the simulation, other than the normal traffic, seven attacks were generated which include Brute Force, Heart Bleed, Botnet, DoS, DDoS, Web, and Infiltration Attack. In this study, the DoS attack was also analyzed. The summary of the dataset is shown in Table 3.

Table 3. Summary of CICDS-2017 dataset.

Filename	Attacks	Number of Samples
Wednesday working hours. pcap	Benign,	440,031
	DoS Hulk	231,073
	DoS GoldenEye	10,293
	DoS Slowloris	5796
	DoS Slowhttptest	5499
	Heartbleed	11

4.2. Data Pre-Processing Steps

The importance of data pre-processing steps cannot be overemphasized since they have a considerable impact on classification performance. We follow a few steps to prepare the data before training the model.

We extract the data of DoS attacks (normal, back, land, neptune, smurf, pod, and teardrop) and normal from the original NSL-KDD dataset to create a new dataset named DoS-KDD which consists of 42 different attributes or columns. We also extract the data of DoS attacks from CICIDS-2017. We consider the Wednesday working hour dataset which contains several kinds of DoS labeled attacks. To develop the deep learning models, all input and output variables are required to be numeric. Since our data are categorical, we encode them to numbers before we fit and evaluate the model. Therefore, we converted non-numerical data to numerical data using 1-to-N encoding such as the protocol TCP is converted to 1, UDP is converted to 2, and ICMP is converted to 3. Subsequently, we remove all constant-valued attributes in all records of DoS-KDD data. These attributes include columns 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21 and 22. This result in dimensionality reduction from 42 to 27 attributes. For DoS-CICIDS-2017, we remove all constant-valued attributes. These attributes include columns 32, 33, 34, 50, 57, 58, 59, 60, 61 and 62. This result in dimensionality reduction from 79 to 69 attributes. The attributes were removed due to their zero value. Lastly, the features in the datasets were normalized to prevent feature differences. The goal of normalization is to change the values of numeric attributes or columns in the dataset into the ranges 0 and 1. We deployed a min-max normalization approach. More information on the min-max normalization can be found in [51].

4.3. Performance Metrics

The performance of the proposed intrusion model was evaluated using the following key metrics; accuracy, precision, recall, and F-score. We present a brief definition of the classification metrics. Accuracy measures the percentage of correct classifications to the total classification made. Precision estimates the probability that a positive prediction is correct. High precision means a low false-positive rate. Recall measures the positive instances that are correctly classified. F-score combines precision and recall. It can be defined as the average value of precision and recall. Mathematically, these metrics can be expressed as [52,53]:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{6}$$

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

$$F - score = 2 \times \frac{(precision \times recall)}{(precision + recall)} \tag{9}$$

where true positives (*TP*) can be defined as the correctly predicted event class or value. False positives (*FP*) happen when the actual class contradicts the predicted one and false negatives (*FN*) can be described as the incorrectly predicted no event values. It happens

when the predicted class contradicts the actual one. True negative (*TN*) can be described as correctly predicted no event values.

5. Results and Discussion

This section presents the results obtained from analyzing the proposed RLSTM model for detecting DoS attacks on the employed IDS datasets.

5.1. Evaluation Results of the Two Datasets

Using the NSL-KDD dataset, Table 4 and Figure 2 presents the results of the proposed model. The results achieved by our proposed model are greater than 0.95 (95%) across all classification metrics. The proposed model accurately classified the attack with a result of 98.6% using the NSL-KDD dataset. With regards to classification error, the proposed model presented a recall and F-score of 98.15% and 98.59%, respectively. The average accuracy, precision, recall, and F-score of 98.60% were achieved from both classification of normal and attack classes. The proposed model predicted 8874 correct classification samples and 126 misclassification samples from the testing data samples.

Table 4. Results of NSL-KDD.

Classifier	Class	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
Proposed RLSTM model	DoS Attack	98.60	99.03	98.15	98.59
	Normal	98.60	98.17	99.04	98.60
	Average	98.60	98.60	98.60	98.60

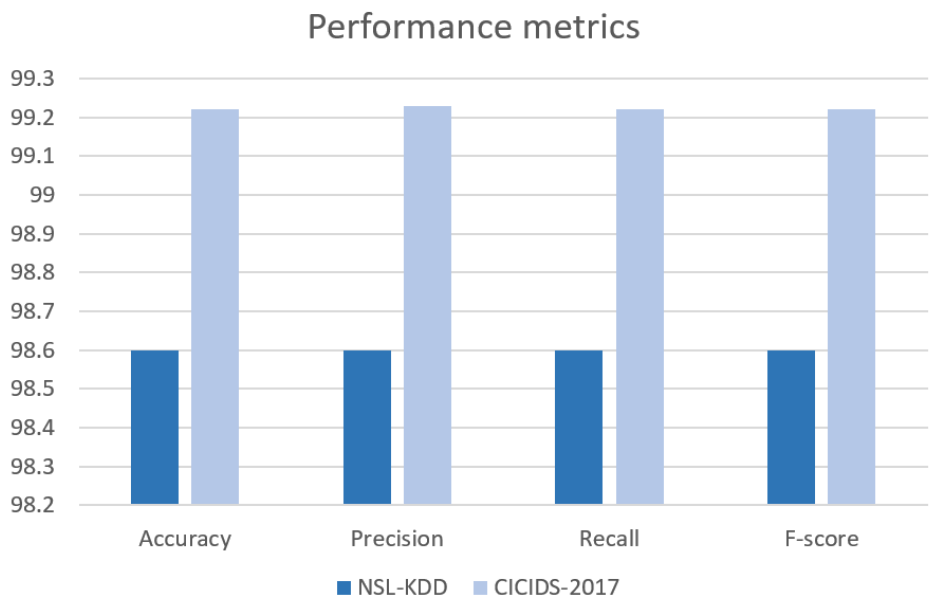

Figure 2. Comparison analysis of the developed RLSTM models using two datasets.

Using the CICIDS-2017 dataset, Table 5 and Figure 2 presents the results achieved from the proposed model. The proposed model accurately classified the DoS attack with a result of 99.22% using the CICIDS-2017 dataset. With regards to classification error, the proposed model presented a recall and *F-score* of 99.62% and 99.22%, respectively. The average accuracy, precision, recall, and *F-score* of 99.22% were achieved from both classification of normal and attack classes. The proposed model predicted 19,250 correct classification samples and 150 misclassification samples from the testing data samples. Overall, the results obtained from the experiments conducted have shown that the proposed model is good at detecting DoS attacks with high accuracy.

Table 5. Results of CICIDS-2017.

Classifier	Class	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
Proposed RLSTM model	Dos Attack	99.2	98.83	99.62	99.22
	Benign	99.2	99.62	98.82	99.22
	Average	99.2	99.23	99.22	99.22

5.2. Comparison with Machine Learning Algorithms

To prove the efficacy of the RLSTM model in terms of feature extraction and classification of intrusions, we compare the model with the most used machine learning algorithm, which is the multilayer perceptron neural network. We choose MLP because of its ability to learn complex relationships, and its ability to easily generalize models and give efficient predictions. The results of the MLPNN classification algorithm for classifying the NSL-KDD and CICIDS-2017 dataset were evaluated and compared with the results achieved from the RLSTM model. Tables 6 and 7 depict the result of the MLPNN model result. The accuracy of the developed RLSTM and MLPNN in correctly classifying the DoS attack is 99.20% and 98.60%, respectively. It could also be observed that the proposed RLSTM model outperformed the developed MLPNN in terms of accuracy and other metrics.

Table 6. Results of MLPNN (NSL-KDD).

Classifier	Class	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
Proposed MLP model	DoS Attack	98.39	98.51	98.27	98.39
	Normal	99.39	99.27	99.51	99.89
	Average	98.89	98.89	98.89	99.14

Table 7. Results of MLPNN (CICIDS-2017).

Classifier	Class	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
Proposed MLP model	Dos Attack	98.22	99.87	96.57	98.19
	Benign	98.22	96.68	99.87	98.25
	Average	98.22	98.28	98.22	98.22

5.3. Performance Comparison with Previous Studies

The proposed model was compared with methods proposed in previous studies. Table 8 presents the comparative analysis of the proposed model results with the results from related works in the literature. Verma et al. [32] proposed and compared different shallow machine learning algorithms including RF, AB, GBM, ERT, CART, and MLP for analyzing samples from CIDDS-001, UNSWNB15, and NSL-KDD datasets and achieved the best results from RF with an accuracy of 94%. Further, Hodo et al. [35] proposed the MLP model which achieved an accuracy of 92.84%. Furthermore, Mohammed et al. [36], proposed and compared DT, k-NN, and NB algorithms. They evaluated their experiments on the CICIDS-2019 dataset and achieved an accuracy of 100%, 98%, and 29%, respectively. Similarly, Susilo et al. [39], proposed RF, MLP, and CNN. Using the BoT-IoT dataset for experimentation, the authors reported CNN as the best model with an accuracy of 91.27%. Ma et al. [40], also presented a CNN model using the NSL-KDD datasets for evaluation. The authors were able to attain a 92.99% accuracy rate. CNN and LSTM model was proposed by Sahu et al. [41]. The authors used the dataset from the Stratosphere lab published in 2020 to evaluate the model and they achieve an accuracy of 96%. When compared to previously proposed methods in the literature, the proposed model performed better in terms of accuracy, precision, recall, and F-score. However, as some of the previously proposed models in the literature used shallow machine learning algorithms, the choice of training parameters and the selected classifiers deployed may have led to different results. Nonetheless, the

proposed model outperforms the models proposed in the literature as they have better feature extraction capabilities, and they perform better with a voluminous dataset.

Table 8. Performance comparison with previous studies.

Classifier	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
RF [32]	94	/	/	/
MLP [35]	92.84	/	/	/
DT, k-NN, NB [36]	100, 98, 29	100, 96, 27	100, 97, 100	100, 97, 42
RF, MLP, CNN [39]	91.27 and 79.01	/	/	/
CNN [40]	92.99	/	/	/
CNN and LSTM [41]	91.20	90.81	92.70	91.75
Proposed model	**99.22**	**99.23**	**99.22**	**99.22**

6. Threat to Validity

This section investigates the validity of the outcomes obtained in this study.

- Construct validity: refers to the relationship between the experiment carried out and the results obtained. This threat is mostly related to the algorithms employed in the experiment. As a result, we were certain that the algorithm's descriptions and pseudocodes employed in this study were correct. The results obtained from the performance metrics in terms of accuracy and other metrics were satisfactory, showing that the proposed model is consistent.
- Internal validity: Internal threats are relatively linked to the experimental setup. Because different parameters must be defined and selected for the algorithm, we employed a grid-search approach to mitigate this threat. The performance metrics employed, and the used dataset are all well-known. As a result, there have been no changes that could have resulted in inaccurate evaluation results.
- External validity: external threats refer to the ability to apply our findings and conclusions to different situations. In this study, the experiments were carried out with two voluminous and popular IDS datasets; NSL-KDD and CICIDS-2017 datasets. Due to the limited availability of real-time IoT network traffic datasets, it should be noted that the two datasets deployed are not generated from typical IoT devices. However, the deployed datasets show similar traits, attributes, and trends of IoT network traffic and recent attack scenarios. In addition, the findings from the work were consistent with what has been found in the literature irrespective of the datasets. In the future, when we model another intrusion detection system, we plan to validate the model using the Bot-IoT dataset which is an IDS dataset designed specifically for IoT.

7. Conclusions

The heterogeneity and ubiquity of the various connected devices, openness to devices in the network, and, importantly, the increasing number of connected smart objects (or devices) have exposed the IoT network to various security challenges and vulnerabilities which include manipulative data injection and cyberattacks such as denial of service (DoS) attack. Any form of intrusive data injection or attacks on the IoT networks can create devastating consequences on an individual connected device or the entire network. In this paper, an intrusion detection system based on RLSTM deep learning technique was proposed for detecting DoS attacks in IoT. The NSL-KDD and CICIDS-2017 datasets were used in the experiments to evaluate the proposed RLSTM model. To improve classification results, the deployed datasets were initially pre-processed before they were used to train the developed RLSTM model. The effectiveness of the proposed model was determined using accuracy, precision, recall, and f-score performance metrics. The proposed RLSTM model achieved 99.22% accuracy for detecting DoS attacks on the CICIDS-2017 dataset. Furthermore, it attained a 99.23% precision rate, 99.22% recall rate, and 99.22% f-score rate for detecting DoS attacks on the CICIDS-2017 dataset. Using the NSL-KDD dataset, the model achieved 98.60% across all the performance metrics. Based on the experimentation

results, it is evident that the RLSTM model proposed has a better intrusion detection effect. The experimental results also demonstrated that the proposed model outperformed the models proposed in the literature. Hence, the proposed RLSTM model can be employed as an intrusion detection system to secure IoT networks from DoS attacks. In future work, we will investigate the possibility of other deep learning algorithms to improve the performance of IDS using the BoT-IoT dataset for IoT security. Furthermore, we plan to investigate other types of attacks against IoT.

Author Contributions: Conceptualization, K.O.A.A., K.O., A.M.A.-M., S.R. and O.A.A.; methodology, K.O.A.A., K.O., A.M.A.-M., S.R. and O.A.A.; software, K.O.A.A., K.O., A.M.A.-M., S.R. and O.A.A.; validation, K.O.A.A., K.O. and A.M.A.-M.; formal analysis, K.O.A.A., K.O. and A.M.A.-M.; investigation, K.O.A.A., K.O. and A.M.A.-M.; resources, K.O.A.A., K.O. and A.M.A.-M.; data curation, K.O.A.A., K.O. and A.M.A.-M.; writing—original draft preparation, K.O.A.A., K.O. and A.M.A.-M.; writing—review and editing, K.O.A.A., K.O., A.M.A.-M., S.R. and O.A.A.; visualization, K.O.A.A., K.O., A.M.A.-M., S.R. and O.A.A.; supervision, K.O. and A.M.A.-M.; project administration, K.O. and A.M.A.-M.; funding acquisition, K.O. and A.M.A.-M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Council for Scientific and Industrial Research, Pretoria, South Africa, through the Smart Networks collaboration initiative and IoT-Factory Program (Funded by the Department of Science and Innovation (DSI), South Africa).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Publicly open-source datasets were analyzed in this study. This data can be accessible at: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 23 May 2021) and https://www.unb.ca/cic/datasets/nsl.html (accessed on 23 May 2021).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ANN	Artificial Neural Network
CART	Classification and Regression Tree
CNN	Convolutional Neural Network
DL	Deep Learning
DT	Decision Tree
DoS	Denial of Service
DDoS	Distributed Denial of Service
ERT	Extremely Randomized Trees
FN	False Negative
FP	False Positive
GBM	Gradient Boosted Machine
IDS	Intrusion Detection System
IoT	Internet of Things
k-NN	k-Nearest Neighbor
RLSTM	Refined Long Short-Term Memory
ML	Machine Learning
MLPNN	Multilayer perceptron Neural Network
NB	Naïve Bayes
NSL-KDD	Network Security Laboratory-Knowledge Discovery in Databases
RNN	Recurrent Neural Network
TN	True Negative
TP	True Positive

References

1. Thamilarasu, G.; Chawla, S. Towards deep-learning-driven intrusion detection for the Internet of Things. *Sensors* **2019**, *19*, 1977. [CrossRef]
2. Evans, D. The Internet of Things: How the next evolution of the Internet is changing everything. *CISCO White Pap.* **2011**, *1*, 1–11.
3. Ray, S.; Jin, Y.; Raychowdhury, A. The changing computing paradigm with Internet of Things: A tutorial introduction. *IEEE Des. Test* **2016**, *33*, 76–96. [CrossRef]
4. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
5. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
6. Cvitić, I.; Peraković, D.; Periša, M.; Stojanović, M.D. Novel classification of IoT devices based on traffic flow features. *J. Organ. End User Comput. (JOEUC)* **2021**, *33*, 1–20. [CrossRef]
7. Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. *IEEE Access* **2017**, *6*, 3619–3647. [CrossRef]
8. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
9. Cvitić, I.; Peraković, D.; Periša, M.; Gupta, B. Ensemble machine learning approach for classification of IoT devices in smart home. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 3179–3202. [CrossRef]
10. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M. A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
11. Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Gener. Comput. Syst.* **2019**, *92*, 265–275. [CrossRef]
12. Adefemi Alimi, K.O.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S. A survey on the security of low power wide area networks: Threats, challenges, and potential solutions. *Sensors* **2020**, *20*, 5800. [CrossRef] [PubMed]
13. Sambangi, S.; Gondi, L. A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression. In Proceedings of the 14th International Conference on Interdisciplinarity in Engineering, Târgu Mureș, Romania, 8–9 October 2020; Volume 63, p. 51.
14. Liu, Z.; Thapa, N.; Shaver, A.; Roy, K.; Yuan, X.; Khorsandroo, S. Anomaly detection on iot network intrusion using machine learning. In Proceedings of the 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 6–7 August 2020; pp. 1–5.
15. Verma, A.; Ranga, V. ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things. In Proceedings of the 4th International conference on Internet of Things: Smart innovation and usages (IoT-SIU), Ghaziabad, India, 18 April 2019; pp. 1–6.
16. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J.; Alazab, A. A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. *Electronics* **2019**, *8*, 1210. [CrossRef]
17. Tang, C.; Luktarhan, N.; Zhao, Y. SAAE-DNN: Deep Learning Method on Intrusion Detection. *Symmetry* **2020**, *12*, 1695. [CrossRef]
18. Thapa, N.; Liu, Z.; Kc, D.B.; Gokaraju, B.; Roy, K. Comparison of Machine Learning and Deep Learning Models for Network Intrusion Detection Systems. *Future Internet* **2020**, *12*, 167. [CrossRef]
19. Jazzar, M.; Hamad, M. An Analysis Study of IoT and DoS Attack Perspective. In *Proceedings of International Conference on Intelligent Cyber-Physical Systems*; Springer: Singapore, 2022; pp. 127–142.
20. Hussain, F.; Abbas, S.G.; Husnain, M.; Fayyaz, U.U.; Shahzad, F.; Shah, G.A. IoT DoS and DDoS attack detection using ResNet. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6.
21. Arnaboldi, L.; Morisset, C. Generating synthetic data for real world detection of DoS attacks in the IoT. In *Federation of International Conferences on Software Technologies: Applications and Foundations*; Springer: Cham, Switzerland, 2018; pp. 130–145.
22. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
23. Leyden, J. Biggest DDoS Attack in History Hammers Spamhaus. The Register, 27 March 2013. Available online: https://www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood/ (accessed on 11 September 2021).
24. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
25. Aminu Ghali, A.; Ahmad, R.; Alhussian, H.S.A. Comparative analysis of DoS and DDoS attacks in Internet of Things environment. In *Computer Science On-Line Conference*; Springer: Cham, Switzerland, 2020; pp. 183–194.
26. Kumar, P.; Bagga, H.; Netam, B.S.; Uduthalapally, V. SAD-IoT: Security Analysis of DDoS Attacks in IoT Networks. *Wirel. Pers. Commun.* **2022**, *122*, 87–108. [CrossRef]
27. Almaraz-Rivera, J.G.; Perez-Diaz, J.A.; Cantoral-Ceballos, J.A. Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. *Sensors* **2022**, *22*, 3367. [CrossRef]

28. Bures, M.; Klima, M.; Rechtberger, V.; Ahmed, B.S.; Hindy, H.; Bellekens, X. Review of Specific Features and Challenges in the Current Internet of Things Systems Impacting Their Security and Reliability. In *World Conference on Information Systems and Technologies*; Springer: Cham, Switzerland, 2021; pp. 546–556.
29. Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors* **2022**, *22*, 1094. [CrossRef]
30. McMillen, D. Internet of Threats: IoT Botnets Drive Surge in Network Attacks. 2021. Available online: https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/ (accessed on 17 December 2021).
31. Balaban, I. Denial-of-Service Attack. *Int. J. Inf. Secur. Cybercrime (IJISC)* **2021**, *10*, 59–64. [CrossRef]
32. Verma, A.; Ranga, V. Machine learning based intrusion detection systems for IoT applications. *Wirel. Pers. Commun.* **2020**, *111*, 2287–2310. [CrossRef]
33. Mohammed, M.M.; Alheeti, K.M. Evaluating Machine Learning Algorithms to Detect and Classify Attacks in IoT. In Proceedings of the International Conference on Communication & Information Technology (ICICT), Basrah, Iraq, 5–6 June 2021; pp. 180–184.
34. Chopra, A.; Behal, S.; Sharma, V. Evaluating machine learning algorithms to detect and classify DDoS attacks in IoT. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021; pp. 517–521.
35. Hodo, E.; Bellekens, X.; Hamilton, A.; Dubouilh, P.L.; Iorkyase, E.; Tachtatzis, C.; Atkinson, R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Hammamet, Tunisia, 11 May 2016; pp. 1–6.
36. Mohammed, S. A Machine Learning-Based Intrusion Detection of DDoS Attack on IoT Devices. *Int. J.* **2021**, *10*, 2278–3091.
37. Cvitić, I.; Peraković, D.; Gupta, B.; Choo, K.K.R. Boosting-based DDoS detection in internet of things systems. *IEEE Internet Things J.* **2021**, *9*, 2109–2123. [CrossRef]
38. Roopak, M.; Tian, G.Y.; Chambers, J. An intrusion detection system against ddos attacks in iot networks. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 562–567.
39. Susilo, B.; Sari, R.F. Intrusion detection in IoT networks using deep learning algorithm. *Information* **2020**, *11*, 279. [CrossRef]
40. Ma, L.; Chai, Y.; Cui, L.; Ma, D.; Fu, Y.; Xiao, A. A deep learning-based DDoS detection framework for Internet of Things. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
41. Sahu, A.K.; Sharma, S.; Tanveer, M.; Raja, R. Internet of Things attack detection using hybrid Deep Learning Model. *Comput. Commun.* **2021**, *176*, 146–154. [CrossRef]
42. Roy, B.; Cheung, H. A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network. In Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 21–23 November 2018; pp. 1–6.
43. Hochreiter, S.; Schmidhuber, J. Long short-term memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef]
44. FatimaEzzahra, L.; Samira, D.; Khadija, D.; Badr, H. Intrusion detection systems using long short-term memory (LSTM). *J. Big Data* **2021**, *8*, 65.
45. Qaddoura, R.; Al-Zoubi, M.; Faris, H.; Almomani, I. A Multi-Layer Classification Approach for Intrusion Detection in IoT Networks Based on Deep Learning. *Sensors* **2021**, *21*, 2987. [CrossRef]
46. Ramotsoela, T.D.; Hancke, G.P.; Abu-Mahfouz, A.M. Behavioural intrusion detection in water distribution systems using neural networks. *IEEE Access* **2020**, *8*, 190403–190416. [CrossRef]
47. Sun, P.; Liu, P.; Li, Q.; Liu, C.; Lu, X.; Hao, R.; Chen, J. DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. *Secur. Commun. Netw.* **2020**, *2020*, 8890306. [CrossRef]
48. Yao, R.; Wang, N.; Liu, Z.; Chen, P.; Sheng, X. Intrusion Detection System in the Advanced Metering Infrastructure: A Cross-Layer Feature-Fusion CNN-LSTM-Based Approach. *Sensors* **2021**, *21*, 626. [CrossRef] [PubMed]
49. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
50. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S.; Alimi, K.O.A. A review of research works on supervised learning algorithms for SCADA intrusion detection and classification. *Sustainability* **2021**, *13*, 9597. [CrossRef]
51. Imrana, Y.; Xiang, Y.; Ali, L.; Abdul-Rauf, Z. A bidirectional LSTM deep learning approach for intrusion detection. *Expert Syst. Appl.* **2021**, *185*, 115524. [CrossRef]
52. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S. Power system events classification using genetic algorithm-based feature weighting technique for support vector machine. *Heliyon* **2021**, *7*, e05936. [CrossRef] [PubMed]
53. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M.; Alimi, K.O.A. Empirical Comparison of Machine Learning Algorithms for Mitigating Power Systems Intrusion Attacks. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–5.