DOI:

Journal of Computers and Intelligent Systems

Vol. 1, No. 1, 2023, pages 27 - 41

Journal Homepage:

https://journals.iub.edu.pk/index.php/JCIS/

DDoS Attack Detection with Deep Learning Algorithm for SNMP, NetBISO, and DNS

Muhammad Imran Ali[1], Asif Raza[2], Sidra Ijaz[3,] Muhammad Asif[4], Hafiz Muhammad Ijaz[5]

[1] Department of Computer Science, Institute of Southern Punjab, Multan Pakistan

[2]Department Computer Science Bahauddin Zakariya University, Multan, Pakistan

[3] Department Mathematics, Government College University Faisalabad, Punjab Pakistan

[4] Department Computer Science & IT, NCBA&E Lahore, Multan Campus, Punjab Pakistan

[5] Department of Computer Science, Institute of Southern Punjab, Multan Pakistan

ARTICLE INFO

Article History:

Received:	February	02, 2024
Revised:	April	25, 2024
Accepted:	April	25, 2024
Available Online:	May	03, 2024

Keywords:

SNMP,
NetBIOS
DNS
LSTM
DDN
Deep Learning

Classification Codes:

Funding:

In this paper, the DNN and the LSTMs methods to find distributed denial of service threats (SNMP, NetBIOS, DNS). With our suggested method, accuracy rates of 99.99% have been reached.

ABSTRACT

In this day and age of advanced technology, devices that are connected to the Internet and can think are a big part of both our everyday lives and the work we do in factories. The number of Internet of Things devices has been steadily increasing from one year to the next, and it is expected that by 2030, there will be 126 billion of them. On the other hand, the number of distributed denial of service, or DDoS, attacks on the Internet's surface has gone up as the number of Internet of Things devices has grown. Because IoT devices are limited in what they can do, it's important to come up with some advanced security techniques to protect the DDoS surface. Because of this, people who want to take control of an Internet of Things device can attack it. This thesis uses the CICDoS2019 dataset to improve how bugs are handled and build a new taxonomy that can handle DDoS attacks better. In the end, this will make the defense against these kinds of attacks stronger. In this paper, the DNN and the LSTMs methods to find distributed denial of service threats (SNMP, NetBIOS, DNS). With our suggested method, accuracy rates of 99.99% have been reached.

Corresponding Author's Email: ImranAli.mltn@gmail.com

Citation:

1. Introduction

In this age of technology, people communicate the most. People need the internet, which is an important part of their lives, to meet this need. People can talk to each other more easily now that the internet is everywhere. The Internet, which is often called the "Internet of things" (IoT), is used more and more in businesses and everyday life. IoT-based connecting devices are small and easy to carry, and they can share information between people without a person being there. [1, 2]. We can use IoT-based devices in our everyday lives, like when we build an intelligent home, factory, or farm. Previous research [3] suggests that by the year 2023, about 125 billion IoT-based devices will be a part of our everyday lives. [Needs citation] On the other hand, IoT-based devices will be more likely to be attacked by DDoS attacks if they don't have low-level security settings. DDoS stands for "distributed denial of service." Because these devices only have a small amount of processing power and memory, they can't stop sophisticated Distributed Denial of Service (DDoS) attacks. Because of this, building or improving Internet of Things base devices that can handle complicated security problems is important and a top priority. If these devices don't get updates, the risk of a distributed denial of service (DDoS) attack may go up, which could affect the Internet of Things base devices that people use. [4,5].

The poisonous truck is on the move, and DDoS attacks have hurt network performance. This means that IoT devices have less bandwidth and resources to use when doing computation tasks. There have been DDoS attacks against the system, which has stopped the services. DoS attacks are talked about in the article [6], which was written by its authors, in a much broader way. The user device has been hit by a series of coordinated attacks, which have taken control of all of the victim's working devices and the system they make up. This kind of attack is called a Botnet DoS attack. In this day and age, the technology behind the internet is changing and getting better, which brings to light some of its problems. More and more DDoS attacks are happening, and they are getting worse. Due to possible weaknesses in their internet domains, a lot of devices used in business, industry, and everyday life could have their users locked out. These holes can cause problems with how the system works, how it handles data, and how much hackers can get paid [7].

DDoS attacks have been affecting our daily lives for a long time. The first distributed denial of service attack happened on July 22, 1999, when a malicious script called Trin00 made its way through the internet and connected to about 114 computers at the University of Minnesota. [8,9]. On October 21, 2016, a problem with their DNS server provider took down GitHub, Twitter, Playstation Server, and several other social and gaming sites. A company that specializes in IT security services said that the attack was linked to the DDoS Botnet [10,11]. GitHub was hit by a DDoS attack on February 28, 2018, with a bandwidth of 1.35 terabits per second and 126.9 million packages per second [12]. This made it hard for the company to run its financial business. According to reports [13], a DDoS attack on a small business (SB) costs about $120,000, while a DDoS attack on a large company costs about $200,000 per attack [14].

At the same rate that the number of Internet of Things devices is growing, so is the number of threads. As a result, industrial businesses are facing new kinds of DDoS attacks, and deep learning (DL) is a key part of the process of finding and stopping these attacks. DL plays a big part in the process of either grouping normal and abnormal features from the dataset together or finding correlations between them. DL also has a lot of work to do to figure out when and where unknown attacks might happen by looking at patterns in data that have already been collected [15,16]. In the past few years, Python has become one of the most popular programming languages because it can use header files. With these files, you can build artificial neural networks much faster than you could before with other languages. Python can also be used to do deep learning.

Unal et al. [17] used the NSL-KDD datasets. The authors of this research used deep learning and a technology called IDS performance to predict a DDoS attack on a network. In this dataset, 41 attributes can be linked to a total of 23 different types of DDoS attacks. Their proposed method works 98.8% of the time, as shown by the evaluation. The people who wrote [18] used the same data set, but they did it in a few different ways. They used Apache Spark's methods to train the model, which brought the accuracy up from 98.8% to 99% and up to 99% overall. A weakness of this work is that they used an older dataset, so their results could have been due to chance, and their model couldn't predict any new attacks.

The CICDDOS219 dataset is being used as part of our investigation. This set of data is made up of information from the Internet of Things devices that we use every day. Here, we use deep learning with the popular classification DNS and the LSTM algorithm.

2. Related Work

The authors of [19] say that if DDoS attacks happen in a network, the first thing that needs to be done for DDoS mitigation is to install a firewall. When DDoS attacks happen, this is always the case. Before doing anything to stop the DDoS attack, the network must first be able to recognize it. The attack can then be stopped. In the past, detecting DDoS attacks in networks was done through the practice of traffic engineering. This was done by building some programmed base rules. Rule-based approaches can't keep up with DDoS attacks because the attacks are so advanced and always changing. Because of this, there need to be some other ways to find these advanced and changing DDoS attacks. So, because of the progress made AI now has a great ability to handle interchangeable attacks. AI is being used by businesses and researchers alike to find new ways to detect DDoS attacks. One thing that makes older methods ineffective is that they can't find risks as well as they could. These problems show up as low accuracy and long wait times. With the help of ML or DL techniques, most backdoor and invisible attack captures can be done much faster and with a much higher level of accuracy.

One of the ways they chose candidate features for classification [20] was by having a human expert do it, and the other was by using a method based on machine learning (ML) [21] to find candidate features. Choosing the right feature to direct DL towards is an important part of the process. DL techniques include both the CNN and the RNN. DL is becoming a more popular way to predict DDoS attacks than other methods.

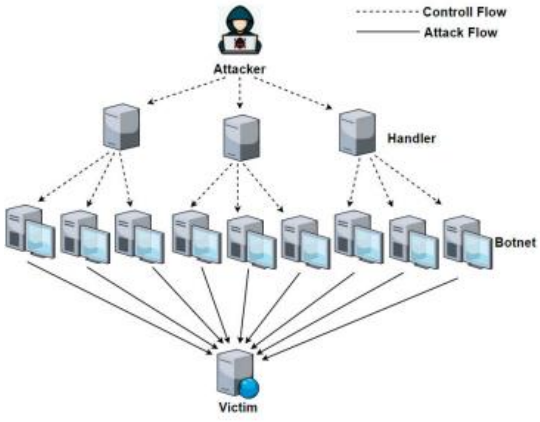


Figure 1 DDoS Attack Example

In [22], the author set up an IP Address Interaction Feature (IAP) model. This model can tell the difference between the normal flow of data in a network and an abnormal flow of data in a network. It also helps find DDoS attacks in a network much faster and more accurately. In earlier studies, most KNN algorithms were able to find incoming data and tell researchers how to classify the incoming data. KNN is a widely used ML classifier method that the authors of [23] used to detect DDoS attacks with the foremost possible result.

Autoencoder is suggested by the authors of [24] as a new way to find DDoS attacks. So, the autoencoder non-label dataset in the algorithm, after that data has been sent to a DNS. During the training phase, this model makes sure that the needed information is kept while ignoring the noise and miner-applicable information from the dataset.

The people who came up with [25] came up with an algorithm called LUCID that used CCN to find DDoS attacks on the network. Compared to other methods or systems that DL has suggested, LUCID saves a lot more time (40 times better). LUCID's preprocessing methods use the dataset-agnostic mechanism and the analysis of activation. Because it works well, LUCID is also a great choice in places with limited resources.

In the article [26], the authors suggest using machine learning algorithms to protect IoT networks from web shell DDoS attacks. Authors use the random forest, extremely randomized trees, and voting as examples of machine learning methods. Voting, (RF), and (ET). According to how the authors grouped the algorithms, the voting algorithm worked much better in both complex and large IoT schemes, while the other two algorithms worked much better in a simple IoT environment.

In [28], two different DL algorithms were used to find DDoS attacks in networks. (LSTM) stood for "Long Short-Term Memory," and (BM) stood for "Bayesian approaches." Most researchers have found that using the LSTM is the best way to find out whether the information is leaving or staying in a network during long-term events and time interval delays. They used to figure out the confidence index for different kinds of DDoS attacks (LSTM). They have used it to show more proof that the attacks have happened (BM)

2.1 Distributed DOS Attack

Computer gadgets are the main source of DDoS attacks in IoT networks or malware infect in IoT devices and attempting to stop running services to the end users. The DDoS attack also prevents the service provider server to shutting its services temporarily. When a large number of IoT devices are inhabited via a Botnet of distribution DDoS attacks happen, but DoS attacks work in a different way of it. Only, if the individual device is present on the internet than flooding DoS attacks happen to IoT devices [29, 30].

2.2 Artificial Neural Network

In the 1950s, the main purpose of the usage of ANN is to perform simple operations such as logical operations. Now, Artificial intelligence is working in multi-disciplined domains such as language transformation, robotics, detection, and recognition. In this age of technology, a large amount of electronic information can be accessed easily. In different businesses, ML and AI have played the main role in resolving potential problems in it. Furthermore, the usage of a (GPU) graphical processing unit can be used to train different algorithms of AI and deep learning (DL) within a couple of seconds such as DNN [31], SVM, and many others.

2.3 Deep Neural Network (DNN) and Long Short Term Memory (LSTM)

A DNN is based on logical regression models, input in the shape of two-dimensional manners. The network of DNN is known as a multi-layered network. There are three types of a layer in DNN, an input layer, one or many hidden layers, and one output layer. If a network has many hidden layers then it's known as DNN. The RNN has suffered escalated gradient issues as well as fade-way gradient problems. The LSTMs algorithm has proposed to reduce the RNN problem by using co-relation between data sets with the help of machine learning and improving to train a model to recognize a DDoS attack in an IoT network [32].

3. Used Approach

Our methodology has been shown in Figure 02. This method has been broken down into five separate steps. The first step is to get the dataset. After that, the dataset needs to go through the preprocessing phase because it will have some empty records and some readings that aren't good for it. In the next step, divide the data set into three parts. In the third step, we have to build the structure of our DNN model and the LSTM method. Both DNNs and LSTM have been taught with the help of the training dataset. Before the actual learning happened, we used a feature selection algorithm to make things easier and reduce the amount of work that needed to be done. After the training, we tried out a few tuning strategies while the validation process was still going on. During the validation process, we were able to find the structure that gives the best answer. After optimizing the structures of the DNN and LSTM algorithms, the suggested method was tested using test datasets.

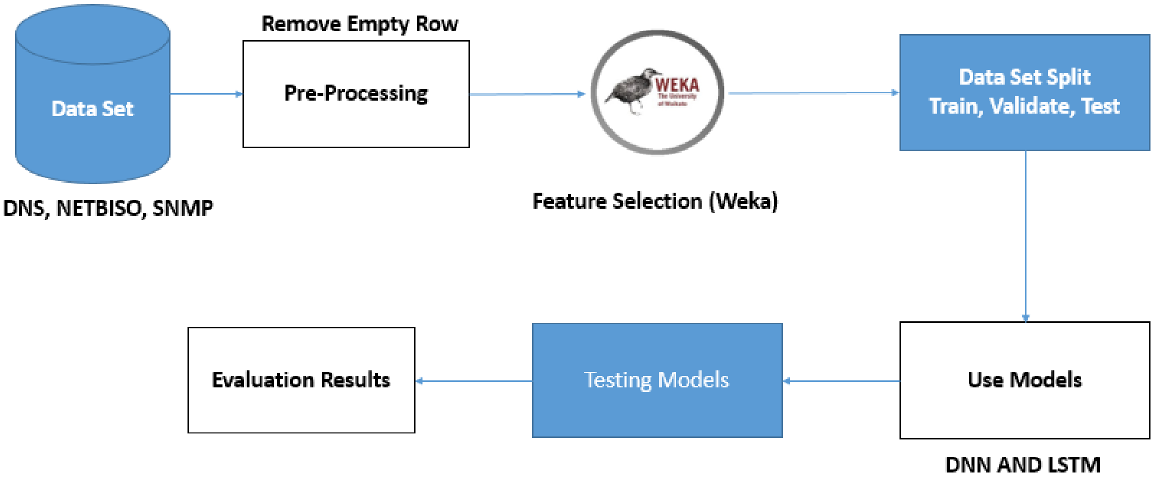


Figure 2 Methodology

3.1 Data Set

The CICDoS2019 dataset is used for this research, and we also made the "DEVELOPING REALISTIC DDoS" dataset of attack and research taxonomies. You can find both of these sets of data here. The publisher of the dataset has added a new type of DDoS attack and shown how growing technology is causing a problem in IoT networks right now. The author of the dataset has suggested several ways to fix bugs and new ways to put things into categories. In addition, they have given suggestions about how to find the most important parts of different DDoS attacks. [33].

3.2 Data preparation

The dataset we used for our models is not good for use in deep learning algorithms as they are now. There will be some records in this dataset that need to be taken out, so there will be some. So, it will move on to the next step, which is preparing the data. In this step of our workflow for processing data, there are three things to do. 1) Cleaning up the data, and 2) deciding which features to use. 3) Planning and making of features.

3.2.1 Data Cleaning

During the data cleansing process, we got rid of all the useless data. Most of the time, this data doesn't exist or it has letters, symbols, and missing attribute values.

3.2.2 Feature Selection

In this step of the process, we use a technique called "feature selection" to pick out only the important part of the DDoS attack. To reach this goal, we used either the Weka tools or the relevant literature from the past to figure out the attributes. This will help us lessen the effects of the DDoS attack that was caused by a feature that has nothing to do with the attack.

3.2.3 Feature Engineering

In the end, we have finally finished using feature engineering on the chosen features to turn them into a form that deep learning can use.

3.3 Dataset Splitting

After the preprocessing step is done, the dataset will usually need to be split into three parts: the training dataset, the testing dataset, and the validation dataset [34].

3.4 3.4 Deep Neural Network

At this point in the process, it's up to us to build the structure of both the LSTM algorithm and the DNN framework. We were able to train a model with this structure with the help of the training dataset. The input layer, the hidden layer, and the output layer are the three layers that make up a DNN. The main job of the input layer is to get data from the dataset, and each neuron in the input layer has its own unique set of traits. The second hidden layer, which is also called the hidden layer, is in charge of getting information from the "input layer" and giving each feature a weight. The very bottom layer is the output layer, and it gets its information from the hidden layer, just like this layer does [35-39]. The output layer is in charge of figuring out what kind of attack is happening. In this case, the chances of each attack have been given different numbers ranging from 0.00 to 1.00. After that comes the next step, which is optimization. At this point in the process, we will use a hyperparameter technique to get better results from the training process. Here, we've changed some algorithm parameters.

4. Implementation

4.3 DataSet Analysis

There are about 46 different properties in the dataset as a whole. Each of these, such as Flow-ID, Source-IP, Source-Port, Destination-IP, Destination-Port, and so on, is called "unnamed." We used the Pandas Profiling Library to look at the dataset and figure out what it meant.

a) Null Values

To finish this task, we need to find the attributes in our dataset that have the "null" value. The goal of this step is to get rid of any values that are blank or have special characters in them. Figure 03 shows the null values in our data set. Using a tool called a "Heat Map," we were able to see the percentage of nulls in the dataset.

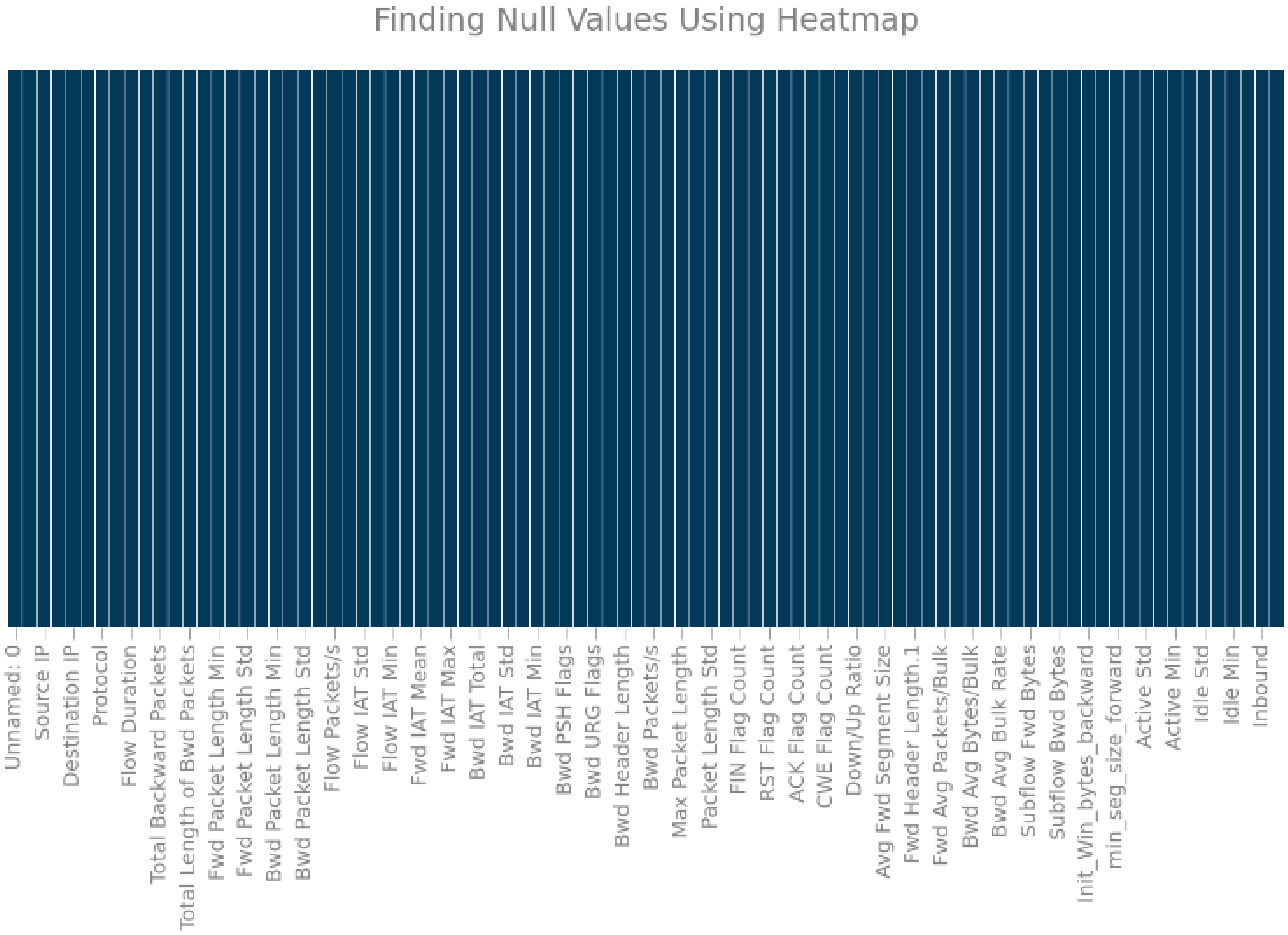
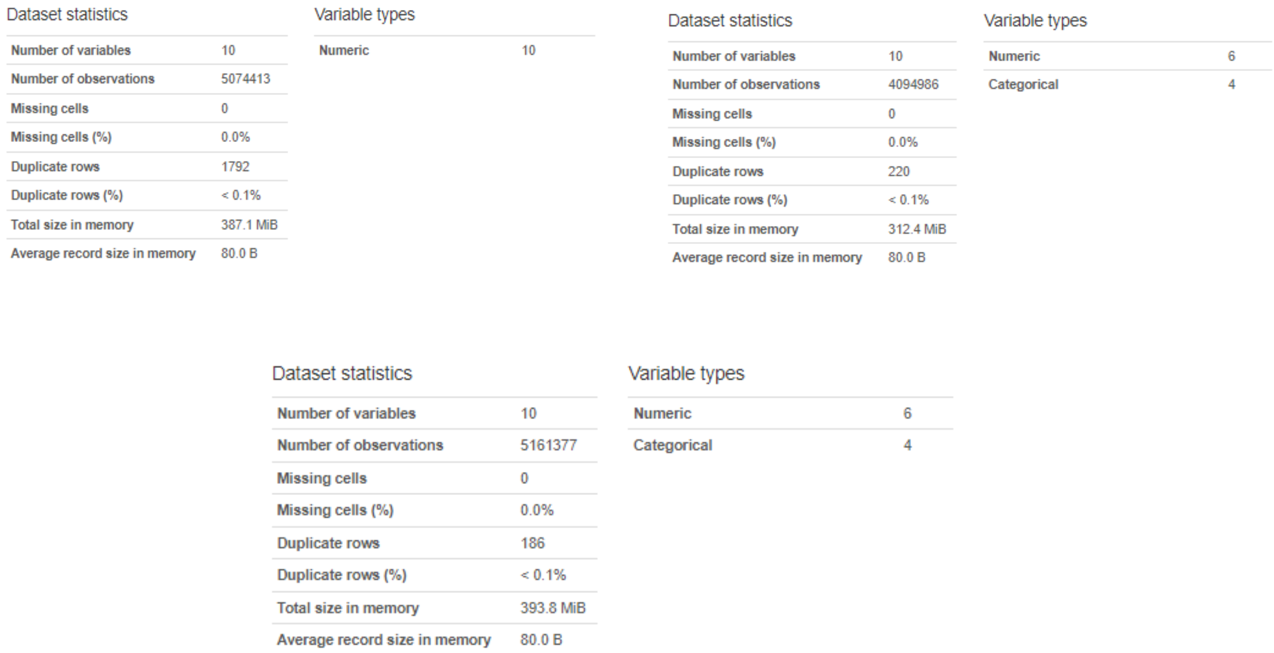


Figure 3 Null Value in Each Data Set

b) Pandas Profiling

- **Overview**

The overview of our data collection revealed that there are no instances of null values within our dataset at all. Following preprocessing, our dataset has a total of ten different attributes. Still there in our data collection are rows that are carbon copies of other rows. Our data collection has a total of 5074413 DNS, 4094.869 NetBIOS, and 5161377 SNMP observations in total. Figure 4 illustrates the fact that each of the 10, and 6:4 properties are Numeric and Categorical respectively datatype.



Dataset statistics

Number of variables	10
Number of observations	5074413
Missing cells	0
Missing cells (%)	0.0%
Duplicate rows	1792
Duplicate rows (%)	< 0.1%
Total size in memory	387.1 MiB
Average record size in memory	80.0 B

Variable types

Numeric	10

Dataset statistics

Number of variables	10
Number of observations	4094986
Missing cells	0
Missing cells (%)	0.0%
Duplicate rows	220
Duplicate rows (%)	< 0.1%
Total size in memory	312.4 MiB
Average record size in memory	80.0 B

Variable types

Numeric	6
Categorical	4

Dataset statistics

Number of variables	10
Number of observations	5161377
Missing cells	0
Missing cells (%)	0.0%
Duplicate rows	186
Duplicate rows (%)	< 0.1%
Total size in memory	393.8 MiB
Average record size in memory	80.0 B

Variable types

Numeric	6
Categorical	4

Figure 4 Overview of each Data Set

c) Correlation within Attributes

To find out how much the DNS dataset's attributes are related to each other. We used that tool to find the Phik correlation coefficient. In the DNS dataset, Packet-LengthStd and Fwd-Packet LengthStd don't have a linear relationship with each other. In the NetBIOS dataset, there is not a straight line between the Bwd IAT Mean and the Bwd IAT Total values. The relationship between the Bwd IAT Mean and the Bwd IAT Total values in the SNMP dataset is not linear Figure 5 shows that all other traits are linked in a straight line, even though none of the other traits have shown a correlation like this.

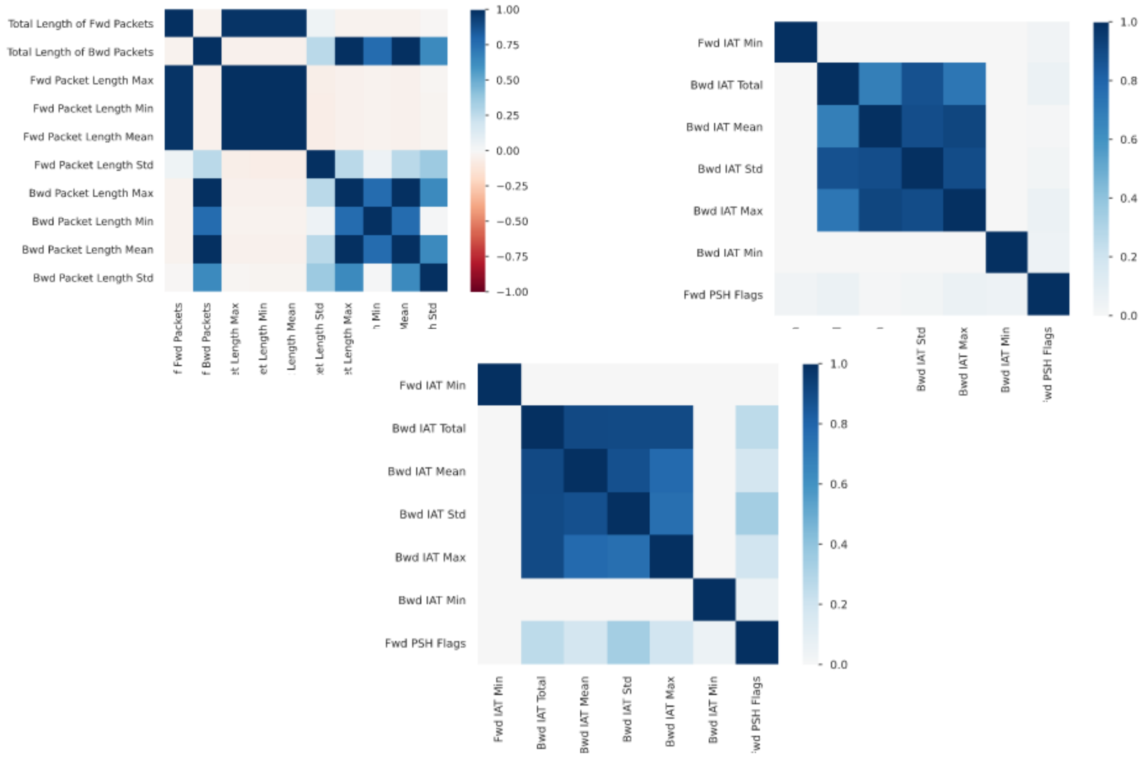
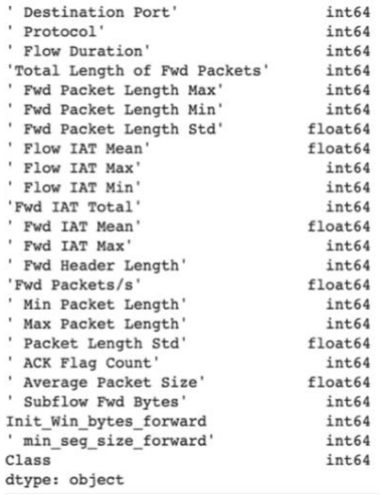


Figure 5 Overview of correlation in each Attribute of the Data Set

d) Feature Selection

To make the DNN and LSTM algorithms less complicated. The weka tool is utilized to pick the candidate features from the DNS data set so that we can reach this goal. Figure 6 shows that the candidate feature was shown after the Weka tool was used. The picture shows very clearly that our dataset has 23 possible features.



```
' Destination Port'                int64
' Protocol'                        int64
' Flow Duration'                   int64
'Total Length of Fwd Packets'      int64
' Fwd Packet Length Max'           int64
' Fwd Packet Length Min'           int64
' Fwd Packet Length Std'         float64
' Flow IAT Mean'                 float64
' Flow IAT Max'                    int64
' Flow IAT Min'                    int64
'Fwd IAT Total'                    int64
' Fwd IAT Mean'                  float64
' Fwd IAT Max'                     int64
' Fwd Header Length'               int64
'Fwd Packets/s'                  float64
' Min Packet Length'               int64
' Max Packet Length'               int64
' Packet Length Std'             float64
' ACK Flag Count'                  int64
' Average Packet Size'           float64
' Subflow Fwd Bytes'               int64
Init_Win_bytes_forward             int64
' min_seg_size_forward'            int64
Class                              int64
dtype: object
```

Figure 6 Overview of feature selection via Weka Tool

5. Evaluation and Results

Deep learning is a framework we made that can find all three types of DDoS attacks mentioned above: DNS, NetBIOS, and SNMP. During the training phase of the model, dropout outliers were used to help limit the amount of overfitting that happened. Dropout has been added to both the DNN and LSTM models so that we can improve our results as much as possible. There are a total of five layers in our DNN model: four dense layers and three dropout layers. There are forty hidden layers, and there are only two output layers. Twenty neurons were used in the first layer. After that, we divided our dataset into three parts: the training dataset, which made up 60% of the whole dataset, the validation dataset, which made up 20% of the dataset, and the testing dataset, which made up 20% of the dataset. Then, we gave our models the training dataset.

We have a ReLU optimizer function that works on all datasets, which lets us find the best hyperparameters for our dataset. During the training process, the ReLU optimizer function was used to change the dataset so that it had a smoother edge. epochs should have a value of 10. Table 1 gives more information about the parameters.

Table 1 Model-Hyperparameter

Identifiers	Values
LossFunction	Spare, CategoricalCrossentropy
ActivationFunction	RELU
Optimizer	ADAM
EpochsSize	TEN
Batchsize	ONE

a) Results

On the test data set, both DNNs and LSTMs perform almost the same. Table 02 shows the F1-Measure, Precision, Recall, and Accuracy of the DNN on three different datasets: SNMP, DNS, and NetBIOS. According to the results, DNN's ability to spot SNMP attacks has gotten **99.97%** better, while its ability to spot DNS attacks has gotten **99.93%** better. Compared to the value of other attacks, DDoS DN's F-Measure is a lot higher. Both the other two types of DDoS attacks are less accurate than the SNMP attack.

Table 2 Performance Metrics (DNN)

Name	Accuracy	Recall	F Measure	Precision
DNS	99.93	1.00	99.95	99.90
NetBIOS	99.96	0.96	99.50	99.42
SNMP	99.97	1.00	99.91	99.97

Based on the DNS, NetBIOS, and SNMP datasets, Table 03 shows the F1-Measure, Precision, Recall, and Accuracy ratings of LSTM. The results showed that LSTM could identify 99.96% of SNMP attacks with the same level of accuracy as DNS attacks. Compared to the value of other attacks, DNS's F-Measure is a lot higher. Both the other two types of DDoS attacks are less accurate than the SNMP attack.

Table 3 Performance Metrics (LSTM)

Data Set Name	Accuracy	Recall	F-Measure	Precision
DNS	99.93	0.97	99.96	99.94
NetBIOS	99.96	0.98	99.65	99.62
SNMP	99.96	0.99	99.93	99.95

Figure 7 shows the results of using DNN and LSTMs. It shows how well the technique worked overall across all datasets. The results show that the overall performance of both algorithms is the same across all three datasets (DNS, SNMP, and NetBIOS).

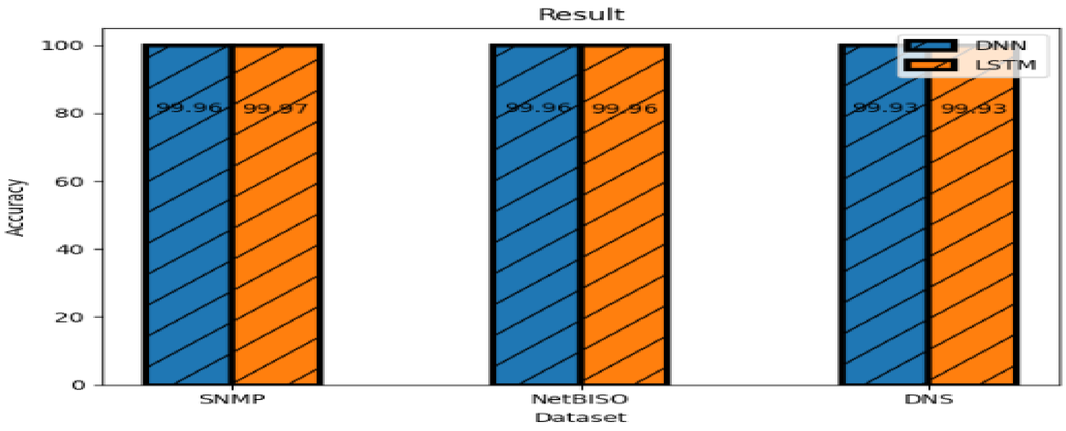


Figure 7 Performance of DNN AND LSTMs on DNS, NetBIOS, SNMP

b) Comparison

In this case, Table 2 shows how the suggested system's model parameters compare to those of the earlier [40]. In older versions of the system, the models used a method called categorical cross-entropy, which can be used for many classes in addition to the target classes. In this case, the values of the probabilities are always moving in either direction. RAdam, which is thought to be more stable and is often used in research, took care of the optimizer function. But in general, RAdam is more successful than regular Adam. The method described in [40] is between 99.93% and 99.95% accurate overall for each of the three types of DDoS attack datasets. After choosing Feature Engineering, all of the attributes can't be used together, so the Sparse Categorical cross-entropy loss function was used in the suggested model. Since the RAdam optimizer worked better than the usual NLP method, it was decided to use it instead of the Adam optimizer in the proposed model. For each of the three types of DDoS attacks, the model's overall performance is between 99.93% and 99.96%. When a few model parameters are changed, this performance is better than [40].

Table 2 Model Parameter for Proposed System AND Previous Ref[40]

No	Ref [40]		Proposed Model
1	**LossFunction**	CategoricalCrossentropy	Sparse, CategoricalCrossentropy
2	**ActivationFunction**	RELU	RELU
3	**Optimizer**	RADAM	ADAM
4	**EpochsSize**	TEN	FIFTEEN

6. Conclusion

The rapid proliferation of Internet of Things (IoT) devices has undoubtedly enhanced various aspects of our daily lives and industrial operations. However, this widespread connectivity also brings about significant security challenges, particularly in the form of distributed denial of service (DDoS) attacks. As the number of IoT devices continues to soar, so does the frequency and intensity of these cyber threats. This paper has addressed the critical need for advanced security measures to safeguard against DDoS attacks targeting IoT devices. Leveraging the CICDoS2019 dataset, we have proposed novel techniques for handling vulnerabilities and developed a comprehensive taxonomy to effectively detect and mitigate DDoS threats. By employing sophisticated methods such as Deep Neural Networks (DNN) and Long Short-Term Memory (LSTM) models, we have demonstrated remarkable accuracy rates of 99.99% in identifying DDoS attack vectors, including SNMP, NetBIOS, and DNS. Our findings underscore the importance of proactive measures in fortifying the defense mechanisms surrounding IoT ecosystems. By enhancing bug-handling processes and implementing advanced detection methodologies, we can bolster the resilience of IoT devices against malicious intrusions. Through continued research and innovation in cybersecurity, we can strive towards a future where the benefits of IoT technology are maximized while minimizing the associated risks posed by cyber threats. In this study, we only looked at three different DDoS attack datasets and used two types of deep learning algorithms: LSTM and DNN. Shortly, we will try to combine several machine learning algorithms and deep learning algorithms so that we can compare how well they work. In addition, we plan to use several different algorithms in our study. Because of this, the results of our research will help find new types of DDoS attacks and solutions to hard problems in IoT networks.

7. References

[1] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, “Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures”, International Journal for Information Security Research (IJISR), vol. 5, no. 4, December 2015, https://doi.org/10.1109/ICITST.2015.7412116.

[2] O. Bello and S. Zeadally, “Intelligent Device-to-Device Communication in the Internet of Things,” in IEEE Systems Journal, vol. 10, no. 3, pp. 1172-1182, Sept. 2016, https://doi.org/10.1109/JSYST.2014.2298837.

[3] M. Miettinen and A. Sadeghi, “Keynote: Internet of Things or Threats? On Building Trust in IoT,” 2018 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Turin, pp. 1-9, 2018, doi: 10.1109/CODESISSS.2018.8525931.

[4] M. Abomhara and G. M. Kien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” in Journal of Cyber Security and Mobility, vol. 4, no 1, pp. 65-88, Jan 2015, https://doi.org/10.13052/jcsm2245-1439.414.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, https://doi.org/10.1109/COMST.2015.2444095.

[6] “The first DDoS attack was 20 years ago,” Emerging Technology from the arXiv. [Online]. Available: https://www.technologyreview.com/s/613331/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learnedsince/

[7] X. Yuan, C. Li and X. Li, “DeepDefense: Identifying DDoS Attack via Deep Learning,” 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, pp. 1-8, 2017, https://doi.org/10.1109/SMARTCOMP.2017.7946998.

[8] J. Smith-perrone and J. Sims, “Securing cloud, SDN and large data network environments from emerging DDoS attacks,” 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, pp. 466-469, 2017, doi: 10.1109/CONFLUENCE.2017.7943196.

[9] Abhishta, R. V. Rijswijk-Deij, and L. J. M. Nieuwenhuis, “Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers,” ACM SIGCOMM Computer Communication Review, vol. 48, no. 5, 70-76, January 2019, https://doi.org/10.1145/3310165.3310175.

[10] H. K. Hyder and C. Lung, “Closed-Loop DDoS Mitigation System in Software Defined Networks,” 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, pp. 1-6, 2018, doi: 10.1109/DESEC.2018.8625125.

[11] “DDoS Breach Costs Rise to over $2M for Enterprises finds Kaspersky Lab Report,” Woburn, MA. [Online]. Available:https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprisesfinds-kaspersky-lab-report/.

[12] Y. Xin et al., “Machine Learning and Deep Learning Methods for Cybersecurity,” in IEEE Access, vol. 6, pp. 35365-35381, 2018, https://doi.org/10.1109/ACCESS.2018.2836950.

[13] Y. Imamverdiyev and F. Abdullayeva, “Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine,” Big Data, vol. 6, no. 2, pp. 159-169, 2018, https://doi.org/10.1089/big.2018.0023.

[14] Y. LeCun, Y. Bengio, and G. Hinton, Deep learning. Nature 521, 436–444, 2015, https://doi.org/10.1038/nature14539.

[15] A. S. Unal and M. Hacibeyoglu, “Detection of DDOS Attacks in Network Traffic Using Deep Learning,” International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES18). http://indexive.com/Paper/157/detection-of-ddos-attacks-in-network-traffic-using-deep-learning.

[16] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet of Things,” Future Generation Computer Systems, vol. 82, May 2018, pp. 761-768, 2017, https://doi.org/10.1016/j.future.2017.08.043.

[17] R. Doshi, N. Apthorpe and N. Feamster, “Machine Learning DDoS Detection for Consumer Internet of Things Devices,” 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, pp. 29-35, 2018, https://doi.org/10.1109/SPW.2018.00013. ISSN: 2252-8938 Int J ArtifIntell, Vol. 10, No. 2, June 2021: 382 – 388 388

[18] Distributed denial of service attack (DDoS) definition.imperva. [Online]. Available: https://www.imperva.com/learn/application-security/ddos-attacks/

[19] K. N. Mallikarjunan, K. Muthupriya and S. M. Shalinie, “A survey of distributed denial of service attack,” 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, pp. 1-6, 2016, https://doi.org/10.1109/ISCO.2016.7727096.

[20] Marchi D. L., and Mitchell L., “Hands-On Neural Networks: Learn how to build and train your first neural network model using Python,” Packt Publishing, 2019.

[21] Farooq, M. U., Khan, S. U. R., & Beg, M. O. (2019, November). Melta: A method level energy estimation technique for android development. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-10). IEEE.

[22] C. D. McDermott, F. Majdani and A. V. Petrovski, “Botnet Detection in the Internet of Things using Deep Learning Approaches,” 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, pp. 1-8, 2018. https://doi.org/10.1109/IJCNN.2018.8489489.

[23] Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” 2019 International Carnahan Conference on Security Technology (ICCST), CHENNAI, India, pp. 1-8, 2019, https://doi.org/10.1109/CCST.2019.8888419.

[24] Workflow of a Machine Learning project. Ayush Pant. [Online]. Available: https://towardsdatascience.com/workflow-of-a-machine-learning-project-ec1dba419b94/

[25] Mahjabin, T.; Xiao, Y.; Sun, G.; Jiang, W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Netw. 2017, 13. [CrossRef]

[26] Genie-Networks. DDoS Attack Statistics and Trends Report for 2020. 2021. Available online: https://www.genie-networks.com/ gnnews/ddos-attack-statistics-and-trends-report-for-h1-2020/ (accessed on 6 May 2021).

[27] Jonker, M.; Sperotto, A.; Pras, A. DDoS Mitigation: A measurement-based approach. In NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium; IEEE: Piscataway Township, NJ, USA, 2020; pp. 1–6.

[28] Priya, S.S.; Sivaram, M.; Yuvaraj, D.; Jayanthiladevi, A. Machine learning based DDoS detection. In Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics, Pune, India, 12–14 March 2020; IEEE: Piscataway Township, NJ, USA, 2020; pp. 234–237.

[29] Yulita, I.N.; Fanany, M.I.; Arymuthy, A.M. Bi-directional Long Short-Term Memory using Quantized data of Deep Belief Networks for Sleep Stage Classification. Procedia Comput. Sci. 2017, 116, 530–538. [CrossRef]

[30] Geng, C.; Huang, S.J.; Chen, S. Recent advances in open set recognition: A survey. IEEE Trans. Pattern Anal. Mach. Intell. 2020, 14, 1–19. [CrossRef] [PubMed]

[31] Cao, A.; Luo, Y.; Klabjan, D. Open-set recognition with Gaussian mixture variational autoencoders. arXiv 2020. Available online: https://arxiv.org/abs/2006.02003 (accessed on 6 May 2021).

[32] Cheng, J.; Yin, J.; Liu, Y.; Cai, Z.; Wu, C. DDoS attack detection using IP address feature interaction. In Proceedings of the IEEE International Conference on Intelligent Networking and Collaborative Systems, Thessalonika, Greece, 24–26 November 2010; IEEE: Piscataway Township, NJ, USA, 2009; pp. 113–118.

[33] Vu, N.H. DDoS attack detection using K-Nearest Neighbor classifier method. In Proceedings of the International Conference on Telehealth/Assistive Technologies, Baltimore, Maryland, USA, 16–18 April 2008; IEEE: Piscataway Township, NJ, USA, 2008; pp. 248–253.

[34] Fadlil, A.; Riadi, I.; Aji, S. Review of detection DDoS attack detection using Naïve Bayes classifier for network forensics. Bull. Electr. Eng. Inform. 2017, 6, 140–148. [CrossRef]

[35] Wang, C.; Zheng, J.; Li, X. Research on DDoS attacks detection based on RDF-SVM. In Proceedings of the 10th International Conference on Intelligent Computation Technology and Automation, Changsha, China, 9–12 October 2017.

[36] Farooq, M. U., & Beg, M. O. (2019, November). Bigdata analysis of stack overflow for energy consumption of android framework. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-9). IEEE.

[37] Khan, S., Khan, S. R., & Raza, A. Alignment Finder: An Interactive Ontology Alignment Framework.

[38] Latif, A., Ambreen, M., Raza, A., Khan, S. U. R., & Khan, S. Impact Of Big Data Analytics And Artificial Intelligence On Talent Management.

[39] Yang, K.; Zhang, J.; Xu, Y.; Chao, J. DDoS attack detection with AutoEncoder. In IEEE/IFIP Operations and Management Symposium; IEEE: Piscataway Township, NJ, USA, 2020; pp. 1–9.

[40] Khempetch, Thapanarath, and PongpisitWuttidittachotti. "DDoS attack detection using deep learning." *IAES International Journal of Artificial Intelligence* 10.2 (2021): 382.