Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Deep learning model for distributed denial of service (DDoS) detection

Chaminda Tennakoon [1,*], Subha Fernando [2]

[1]Department of Computing, Informatics Institute of Technology, Colombo, Sri Lanka
[2]Department of Computational Mathematics, University of Moratuwa, Moratuwa, Sri Lanka

ARTICLE INFO

Article history:
Received 27 August 2021
Received in revised form
8 December 2021
Accepted 15 December 2021

Keywords:
Application-layer
DDoS detection autoencoder
Deep learning models
Cybersecurity

ABSTRACT

Distributed denial of service (DDoS) attacks is one of the serious threats in the domain of cybersecurity where it affects the availability of online services by disrupting access to its legitimate users. The consequences of such attacks could be millions of dollars in worth since all of the online services are relying on high availability. The magnitude of DDoS attacks is ever increasing as attackers are smart enough to innovate their attacking strategies to expose vulnerabilities in the intrusion detection models or mitigation mechanisms. The history of DDoS attacks reflects that network and transport layers of the OSI model were the initial target of the attackers, but the recent history from the cybersecurity domain proves that the attacking momentum has shifted toward the application layer of the OSI model which presents a high degree of difficulty distinguishing the attack and benign traffics that make the combat against application-layer DDoS attack a sophisticated task. Striding for high accuracy with high DDoS classification recall is key for any DDoS detection mechanism to keep the reliability and trustworthiness of such a system. In this paper, a deep learning approach for application-layer DDoS detection is proposed by using an autoencoder to perform the feature selection and Deep neural networks to perform the attack classification. A popular benchmark dataset CIC DoS 2017 is selected by extracting the most appealing features from the packet flows. The proposed model has achieved an accuracy of 99.83% with a detection rate of 99.84% while maintaining the false-negative rate of 0.17%, which has the heights accuracy rate among the literature reviewed so far.

1. Introduction

In the cutting-edge web age industries like e-commerce, banking, news, social networking, and plenty of many more conveyed their services through the Internet. Disrupting the common accessibility of a system for its legitimate users is called the Denial of Service (DoS) attacks.

The Distributed Denial of Service (DDoS) attacks are a type of DoS attacks carried out by multiple infected series of IP addresses that can be span over massive geographical locations. The DDoS attacks disrupt the regular traffic of a service like a business server or website by overwhelming the particular target with an array of Internet traffic (Chio and Freeman, 2018). Zombies and Botnets are utilized to dispatch DDoS attacks that can cause genuine harm to a business organization's operability and accessibility by its operations to shut down or slow down. In the competitive global business world, these slow down or shut down can seriously damage the business growth and its reputation. Political, Economic, Cybercrime, and Terrorism are the motives for DDoS attacks.

The year 2002 is the first recorded DDoS (Norton, 2020) attack, and there were many such incidents recorded after that. The DDoS attack on domain name provider DYN in the year 2016 was a massive one where it crippled leading web-based businesses like CNN, Airbnb, Netflix, The New York Times, Spotify, Amazon, GitHub, PayPal, Reddit, and Visa (Norton, 2020; Asad et al., 2020). The Mirai botnet was responsible for carrying out the attack that exploits the weakness found within the IoT devices. The attack reflected that these DDoS attackers used evolving strategies to achieve massive bandwidth (Petters, 2019).

Based on the DDoS taxonomy depicts in Fig. 1, there are two main types of DDoS attacks as Reflection and Exploitation (Sharafaldin et al., 2019).

* Corresponding Author.
Email Address: chaminda.2019188@iit.ac.lk (C. Tennakoon)
https://doi.org/10.21833/ijaas.2022.02.012
Corresponding author's ORCID profile:
https://orcid.org/0000-0001-9804-8560

The reflection type of DDoS keeps the identity of the attacker hidden by utilizing the legitimate third party to carry out the attack. These types of attacks are carried out through the application layer protocols with the aid of transport layer protocols such as Transmission control protocol (TCP), User datagram protocol (UDP), or both. The exploitation DDoS attacks are very similar to the reflection attacks where the identity of the attacker remains hidden. These types of attacks are utilizing both TCP and UDP to carry out an attack. SYN flood, UDP flood, and UDP lag are fallen into the exploitation attack category.

The DDoS attacks can be seen targeting the Transport layer and Network layer of the OSI model. Now it has shifted to the application layer as well that perceived to be sophisticated and provides greater challenges when dealing with it (Asad et al., 2020). The DDoS attackers have ceaselessly rummaged around for new vulnerabilities so that they alter their way of attacking from one attack to another. These evolving various attacking strategies have the trend of inclined frequency of DDoS attacks as well as the magnitude of such attacks. The DDoS attack forecasted from the year 2018 to 2023 is depicted in Fig. 2 and it demonstrates that the number of DDoS attacks from each year keeps increasing (Cisco, 2020).

Infrastructure approaches like Firewalls and Load balancers are been used to mitigate the DDoS attacks, but provide their own limitations. Both firewalls and load balancers are stateful inline solution devices that are vulnerable to state-exhausting attacks. Therefore, they are limited and partial solutions for the customers who are demanding best-of-breed DDoS protection. Further to infrastructure approaches, anomaly-based, and signature-based (Gupta, 2018) approaches have been employed for DDoS detection. The signature-based way of detection is likely to be obsolete quickly. Anomaly-based detection has a higher rate of false-positive. So, both approaches present the reliability issues of such detection solutions. To prevent or minimize the DDoS attack damage the false positive and false negative rates need to be kept at near-zero.

The most recent drift in identifying DDoS assaults is utilizing Machine Learning (ML). The capacity to adjust or change the approach as the information evolves is the strength of the ML. It can be seen that both unsupervised and supervised models have been utilized for DDoS detection approaches. Since the batch stream carries the majority of the negative class, to detect the DDoS attack, accuracy alone cannot be used as the measurement criteria. Therefore, while maintaining the high accuracy rate, the key is the recall rate of the DDoS. Indeed, in spite of the fact that the machine learning approaches are exceptionally prevalent in many of the DDoS detection models. But the main obstacle is to take care of false-positive to close zero while maintaining the high recall rate for the DDoS discovery.

The application-layer DDoS detection model proposed by this study is based on the deep learning techniques utilizing the capabilities of Autoencoder and the Deep neural network. The packet information related to traffic flow from a network adaptor captures through the PCAP file and significant features are identified by using the packet parsing techniques. The autoencoder is used for the feature extraction before being fed into the deep neural network model for classification. The new feature vector generated by the autoencoder fed into the deep learning model for final prediction. The proposed model has achieved an accuracy rate of 99.83% with a detection rate of 99.84%. Further to that model was able to achieve a low false alarm rate which is key for any detection model. Model's false positive rate is recorded as 0.18% while maintaining the false-negative rate at 0.17%. To evaluate the developed model, GANs were designed to simulate the future DDoS attack and the proposed model was able to detect those unseen attacks. This study has achieved the accuracy of the height against the dataset CIC DoS 2017 dataset as per the current literature review.

The rest of the paper is organized as follows. In section two, the paper discusses the background theories very briefly. Section three discusses past approaches with regards to DDoS detection using machine learning approaches and section four describes the proposed solution while section five describes how the experiment was done. The results obtained are discussed in section six. Finally, the conclusion and possible future enhancements are discussed in section seven.

2. Background theories

2.1. Deep learning

Natural Language Processing and Computer Vision have a noteworthy impact from Deep Learning approaches.

Containing many layers to learn from, identifying the significant feature set from the feeding data, and on top of it adjusting capability with the novel data are key characteristics of the Deep learning models (Bediako, 2017).

2.2. Autoencoder

Working with datasets that contain hundreds of features is becoming common nowadays where the number of observations in a dataset sometimes leads to a machine learning model to be suffering from overfitting (Ippolito, 2019). Regularization and dimensionality reduction are the techniques that have been employed to overcome the overfitting problem of machine learning. Creating new features by reducing the number of features in a dataset is called feature extraction.

Autoencoder is a specific type of feedforward unsupervised learning technique in which seeks to

learn from a compressed representation (Jordan, 2018; Rupak, 2020).

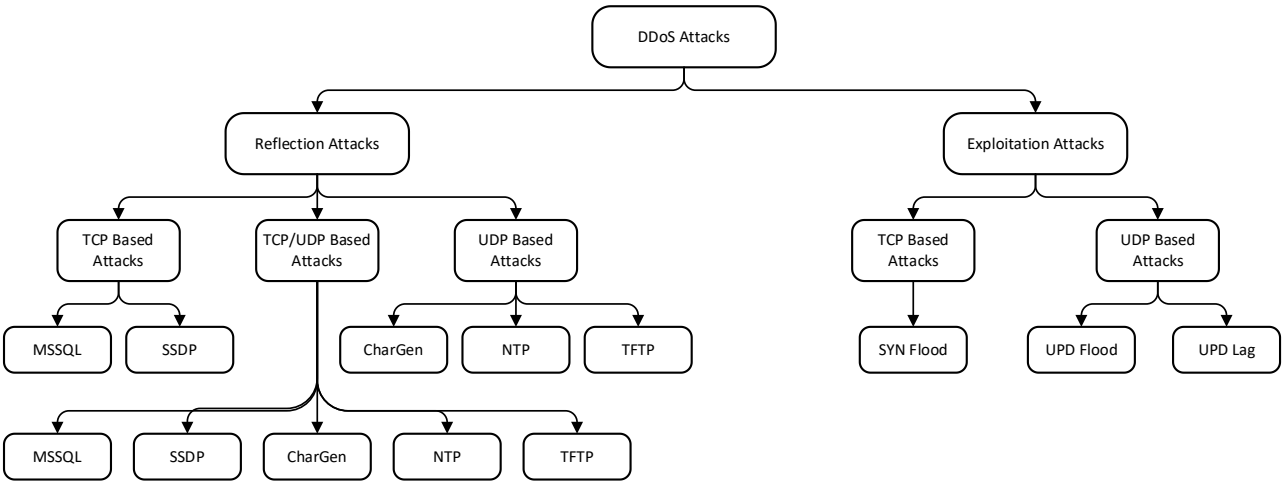

Fig. 1: DDoS attack taxonomy (Sharafaldin et al., 2019)

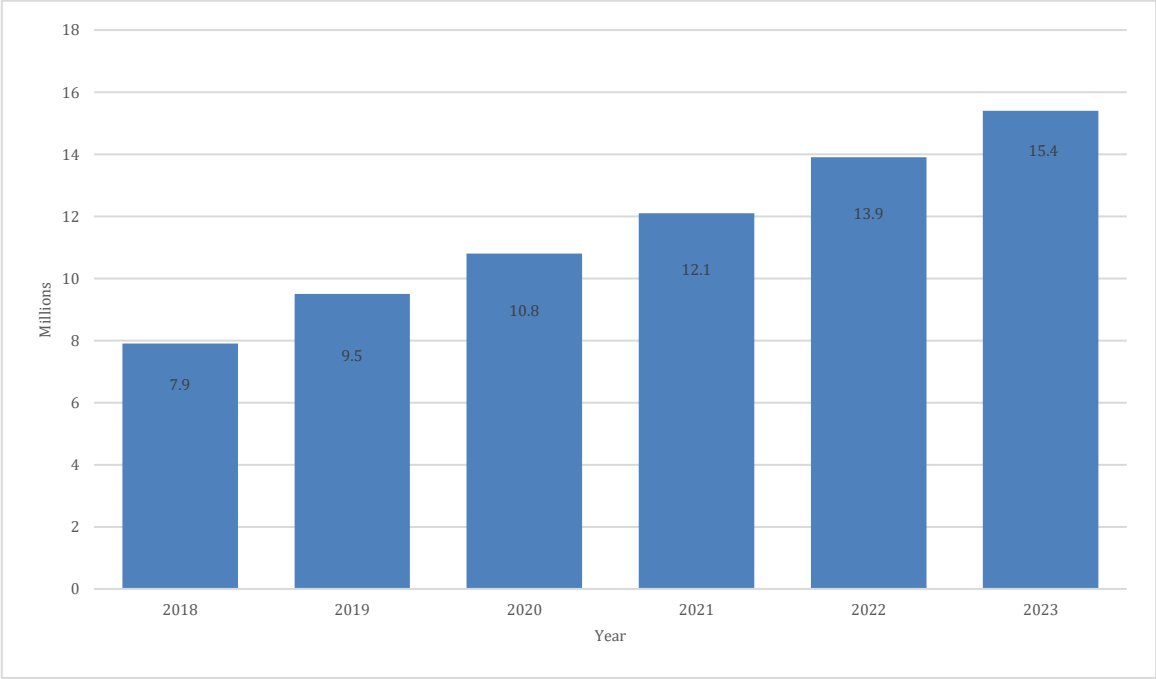

Fig. 2: Number of DDoS attacks forecast (Cisco, 2018)

The autoencoder contains three components as encoder, code, and decoder where the autoencoder compresses the input into lower-dimensional called code and reconstructs the output from this code representation (Dertat, 2017).

There are many types of autoencoders are available that suited different types of scenarios. But the common usage of autoencoders is for feature extraction or dimensionality reduction. Fig. 3 demonstrates the basic structure of an autoencoder model (Rupak, 2020).

2.3. Generative adversarial networks (GANs)

The GANs are neural network architecture which is generative models that are capable of producing or generating new content that resembles the training data. The generation of new data/content hugely benefited the data-limited situations as well as generating a new pattern of data. GANs have two components as generator and discriminator. The generator generates the data while the discriminator determines whether the generated data looks real or not. So, the two networks compete with each other to improve the realistic nature of the generated data (Nash, 2019) and Fig. 4 shows how the basic flow of generative adversarial networks works.

3. State of the art

It can be seen that many of the researchers have done their research using machine learning approaches to build models to detect DDoS attacks accurately. Especially the deep learning techniques fashionable among those researchers. As per the latest findings, Asad et al. (2020) from their research proposed a model to detect application-layer DDoS attacks, and the model was based on a seven-layer Deep Neural network with feed-forward and back-propagation. They used batch normalization at the

input layer by scaling and adjusting the activation function which they argue as their novelties of the model. The Min-Max scaling technique was selected based on the performance and the model evaluated against the dataset CIC IDS 2017. The proposed model was able to achieve an F1 score of 0.99.

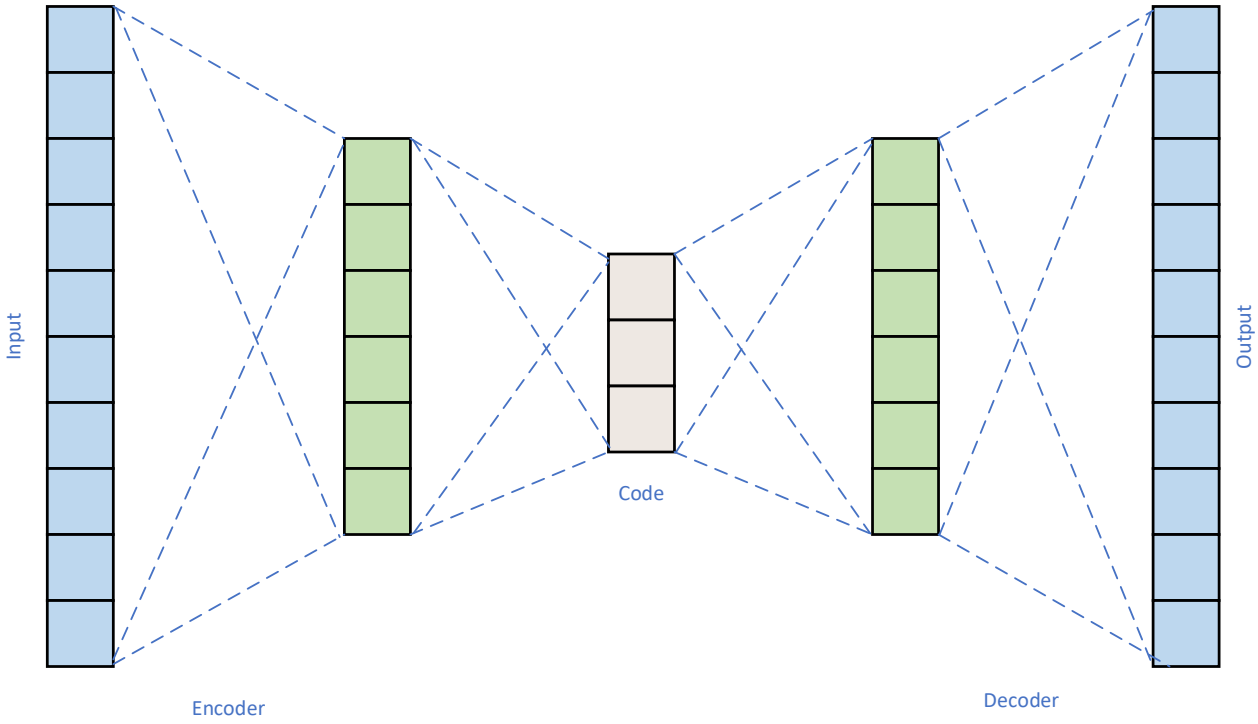

Fig. 3: Autoencoder model (Rupak, 2020)

Kim (2019) proposed a supervised learning approach to detect DDoS attacks using a basic neural network and LSTM using Tensor Flow for feature extraction. Both pre-processing methods and hyperparameters optimization were investigated against three datasets which are CAIDA, DARPA, and dataset collected by Alkasassbeh et al. (2016). The Box-Cox transformation and min-max transformation methods were used for pre-processing. From the research Kim (2019) argued that for the DDoS detection pre-processing methods, neural network architecture and hyperparameters, and the optimizers are appropriate.

Revathi and Malathi (2014) proposed a DoS attack detection model using Random Forest (RF) classifier, and Principal Component Analysis (PCA). The dataset NSL-KDD was used and applied PCA to reduce attributes to avoid dimensionality problems. The reduced 14 attributes were used for the classification in the RF classifier. In the research, Revathi and Malathi (2014) used the Weka tool for experimental analysis and were able to achieve 99.9% accuracy. Filho et al. (2019) from their research proposed a model with an RF Tree algorithm that classified network traffic based on samples taken from the sFlow protocol directly from the network devices. After the performance calibration, the model was evaluated against three benchmark datasets CIC-DoS, CIC IDS 2017, and CSE-CIC-IDS2018. The evaluation demonstrated an accuracy rate of 93%.

A model that consists of the stacked autoencoder and One-class SVM (SAE-1SVM) was proposed by Mhamdi et al. (2020). The main focus of Mhamdi et al. (2020) was to handle an imbalanced dataset that is the common case of most of the datasets that are available for DDoS detections. The size similarity can be observed from both encoder and decoder in the Autoencoder proposed by Mhamdi et al. (2020). On the other hand, OC-SVM is an unsupervised learning approach that tries to learn a hyperplane that best separates all the data points in the origin. CIC IDS 2017 dataset was used as the benchmark dataset for their research. Even though Mhamdi et al. (2020) demonstrate 99.35% accuracy, their false positive rate was quite high.

A comparison study conducted by Wankhede and Kshirsagar (2020) used Multi-Layer Perception (MLP) neural network and RF with the use of the benchmark dataset CIC IDS 2017 with the help of the Weka tool concluded that RF outperformed MLP with the accuracy of 99.95%.

In the past, most of the significant researchers were based on KDD CUP 1999 dataset (Table 2). Imamverdiyev and Abdullayeva (2018) conducted their study on the application of the deep learning methodology-based Gaussian-Bernoulli type restricted Boltz-Mann machine (RBM) to DDoS detection. To achieve higher detection accuracy, during the training the hyperparameters were adjusted. SVM (epsilon-SVR), Decision Tree, Deep belief network, Bernoulli-Bernoulli RBM, Gaussian-Bernoulli RBM, and SVM radial basis models were used for comparative study by Imamverdiyev and Abdullayeva (2018) and concluded that the multilayer deep Gaussian-Bernoulli RBM is a better

model than other models that selected for comparative study and used the NSL-KDD as the experiment dataset. Kale and Choudhari (2014) from their comprehensive set of evaluations that used the KDD CUP 1999 dataset argued that Resilient Back Propagation (RBP) is the best classifier. Further optimization was done to improve the RBP performance by combining Neyman Pearson cost minimization strategy and ensemble of classifier output. For their simulation experiments, DARPA 1999, CONFICKER, and DARPA 2000 were used. The model that was based on the Genetic Algorithm proposed by Paliwal and Gupta (2012) to detect DDoS attacks with the help of dataset KDD CUP 1999, was able to record 97% intrusions detection accuracy. Douligeris and Mitrokotsa (2004) from their study form a model to detect DDoS attacks based on Kohonen's Self-Organizing Maps (KSOMs). There was a limitation of the proposed model that the demand of high computational power when the dataset exceeds the number of records 10,000. For the model experiment, they used the dataset KDD Cup 1999.

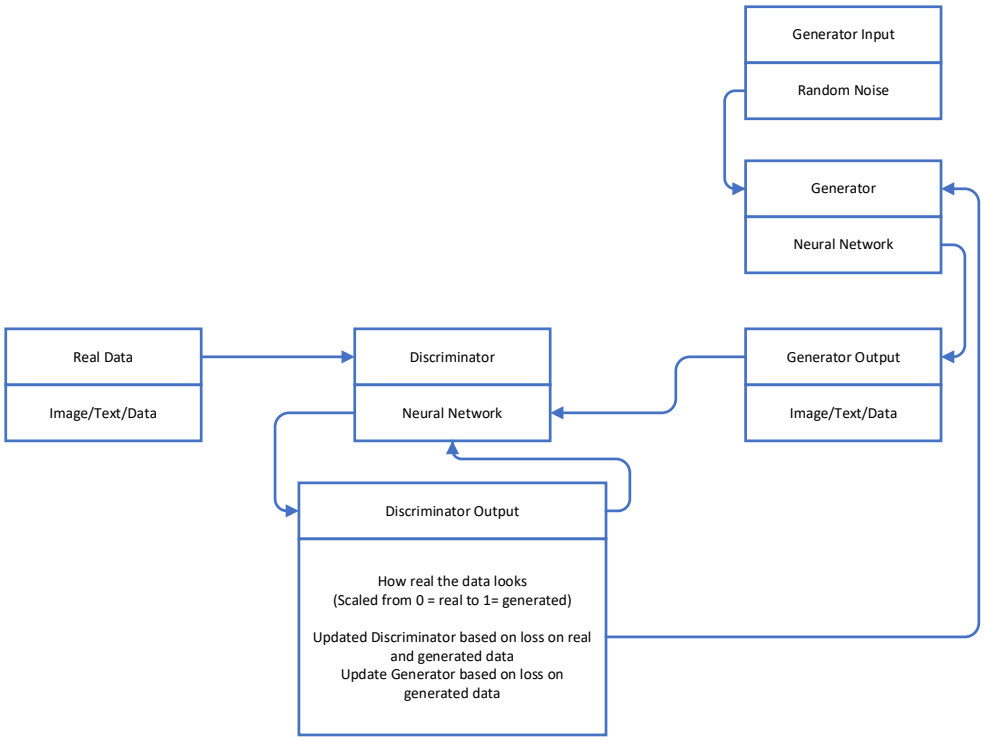

Fig. 4: Generative adversarial networks (Nash, 2019)

In the recent past literature, a different approach has been proposed by Noh et al. (2003) where they employed a traffic analysis mechanism based on ratio calculation. The ratio was formed by the number of flag TCP to the total of TCP packets. The particular ratio was then used for DDoS detection by using state-action rules with the help of the ML algorithm. Noh et al. (2003) used their own simulated network environment for the model experiment. Reinforcement Learning-based based on Q-Learning was proposed by Phan et al. (2019) from their research study which utilized the MaxiNet emulation framework for runtime evaluation of the model. By applying an optimal policy from the Q-Learning agent the model was able to achieve higher DDoS detection performances.

4. Proposed solution

4.1. Overview of the solution

The overview of the proposed solution depicts in Fig. 5. The packet information flows in and out from a network adapter can be captured through a PCAP file. The PCAP file that contains mentioned packet information is the data source for the proposed solution. The PCAP file contains many packets and those packets are analyzed using the PCAP Extractor before being fed into the autoencoder for feature extraction. The feature vectors generated from the autoencoder are used as the input to the detection model for classification as benign or DDoS attacks. The solution contains three main components as PCAP Extractor, Autoencoder, and Detection model.

4.2. Attribute extraction–PCAP extractor model

The packets that are flowing in and out from a network adaptor can be captured through a PCAP file. A given PCAP file contains many packets. The information contains in a stream of packets of one specific connection between source IP and destination IP provides attributes that aid to describe the nature of the connection. There are many packets parsing techniques available. This research has used the concept employed with the pyFlowMeter to build the PCAP extractor model that enables packet parsing and understanding the

significant attributes. The PCAP extractor was able to identify 56 such attributes. The identified features from the PCAP extractor model are then fed into the Autoencoder model. Fig. 6 shows the proposed network architecture for the detection model.

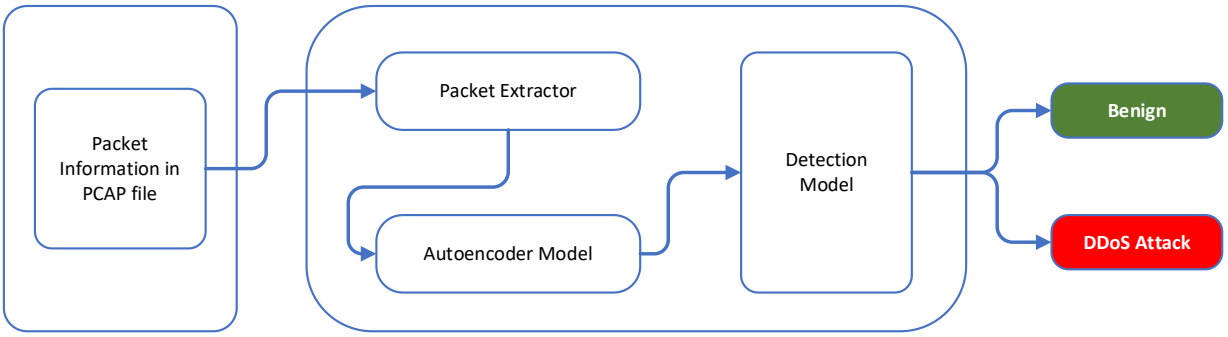

Fig. 5: Proposed solution to detect application-layer DDoS attacks

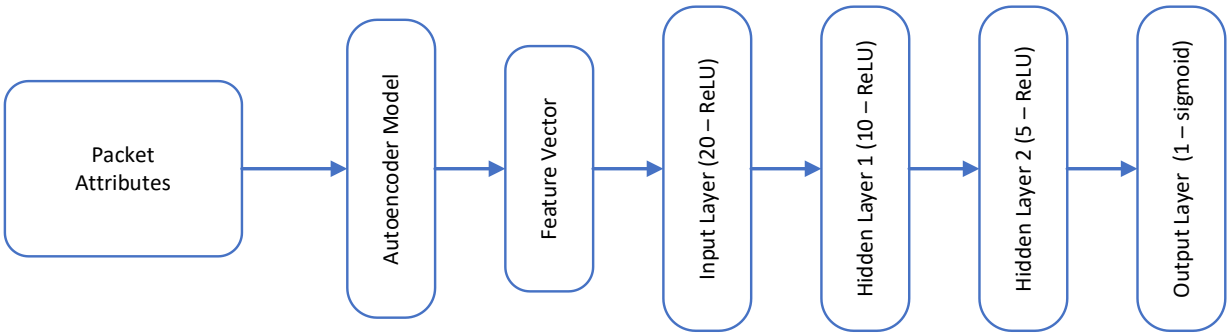

Fig. 6: Proposed network architecture for the detection model

4.3. Autoencoder model

The attributes that are extracted from the PCAP extractor model are fed into the autoencoder to perform the feature extraction. The encoder part of the autoencoder has the input shape of 51 which is equal to the number of features in the dataset after dropping insignificant attributes. The input later contains 27 neurons. The last layer of it has 20 neurons which is the end dimension. The decoder section of the autoencoder is designed with 20 neurons and the output layer with 51 neurons. For all the layers in the autoencoder, it has used ReLU as the activation function.

4.4. Detection model

The DDoS detection model is built using deep neural networks with four dense layers. The features extracted from the autoencoder are used as the input shape of the initial layer of the deep neural networks with 20 neurons. The remaining three layers contain 10, 5, and 1 neuron respectively. Fig. 6 shows the network architecture for the proposed model. The initial layers of the model use ReLU as the activation function while the output layer uses sigmoid as the activation function. The early stopping technique is used to judge the best number of epochs that the model should train.

For the hyperparameter tuning, it is decided to use the trial and error approach since the particular approach provides more insight about the given parameter adjustment and its output result rather than the grid search approach for the purpose. Batch size, weight initialization, activation function, optimization function, learning rate, and loss function are adjusted during the experiment and their results are compared. The final deep neural architecture is implemented using the hyperparameters given in Table 1.

5. Experiment and evaluation

5.1. Experiment environment

The experiment is performed on an Asus machine with Core i7–8550U CPU @ 1.8GHz, 16GB memory. The TensorFlow open-source library with Keras in the python language environment is used for all the implementation.

Table 1: The hyper parameters for the detection model

Variable	Parameter
Optimization Function	Adam
Weight Initializer-Initial Layers	he_normal
Weight Initializer-Other Layers	glorot_normal
Loss Function	hinge
Activation Function-Dense Layers	ReLU
Activation Function-Output Layer	sigmoid
Batch Size	512

Table 2: Publicly available intrusion detection datasets

Dataset	Remark	OSI Layer
ISCX 2012	Generated in 2012 and contains various types of attacks like SSH brute force, DoS or DDoS	Network and Transport
IRCS	Dataset recorded in 2015 and manual inspections were used for labeling	Network and Transport
DDoS 2016	Generated using network simulator NS2 in 2016	Network
CIC IDS 2017	Contains a wide range of attack types like SSH brute force, heart-bleed, botnet, DoS, DDoS	Transport and Application
CIC DoS 2017	Contains only application-layer DDoS attacks on web services like Slowlories, hulk, RUDY, Goldeneye, ddossim, Slowhttptest. The traffic was labeled using pyFlowMeter	Application
CIC DoS	Application layer DoS attacks which combined with ISCX 2012 dataset	Application
DARPA 1998/1999 Includes various types of attacks like DoS, Buffer overflow, Port scans		Transport
KDD CUP 1999	KDD CUP 99 is based on the DARPA dataset and contains more than 20 different types of attacks	Transport
CIC DoS 2019	Contains recent DDoS attacks resembling real data(PCAP) and analysis of the network traffic done using CICFlowMeter. Also, traffic was labeled	Network and Transport

5.2. Benchmark dataset–CIC DoS 2017

Many intrusion detection datasets are publicly available. But it is important to understand their strengths and weaknesses as well as their validity to the current context. Table 2 provides the information about the key benchmark datasets that are identified from the literature reviews (Behal and Kumar, 2016; Jazi et al., 2017).

The study aimed to build a machine learning model to detect application-layer DDoS attacks. Hence when selecting the benchmark dataset, the priority was given to whether the traffic contents were generated purely using the application layer DDoS attacks so that data prep reparation can be kept at the minimum level. In addition to that, the dataset's age is also given the weightage due to the fact of the importance of having the latest attack patterns. Most of the datasets that are listed under Table 2, were containing mixed attack types. Not purely the application layer attacks. But CIC DoS 2017 contains only the application layer DDoS attacks (Jazi et al., 2017), which is matching the purpose of the study.

Further to that, there are many variants of application-layer DDoS attacks have used while creating the CIC DoS 2017 dataset (Jazi et al., 2017) that helps the proposed model to learn from different application-layer attacking patterns. Table 3 shows the different type of application layer attack labels consists in the dataset. Therefore, considering all these positive points. CIC DoS 2017 dataset is selected as the benchmark dataset for the study.

Table 3: Traffic labels in CIC DoS 2017 dataset

Label	Number of Records
Benign/None Label	114,493
ddossim	40,972
slowheaders	7,945
Slowread	4,252
rudy	2,078
slowloris	2,048
hulk	1,934
goldeneye	1,308
slowbody2	1,214

5.3. Performance metrics

The model predicts whether the network traffic is benign or a DDoS attack. Therefore, the confusion matrix is used to analyze the results obtained during the experiment analysis. The confusion matrix applicable to the study is shown in Table 4.

Table 4: Confusion matrix for the study

		Predicted Classe	
		Benign	DDoS
Actual Classes	Benign	TN	FP
	DDoS	FN	TP

True Positive (TP): The count of incoming DDoS attacks were classified correctly

True Negative (TN): The count of normal traffic classified correctly

False Positive (FP): The count of normal traffic was classified as a DDoS attack

False Negative (FN): The count of DDoS attacks was classified as normal traffic

In addition to that, standard measurements like accuracy, precision, and f1-score are used for the model evaluation. The confusion matrix statistics are used to calculate different indicators about the model performances based on the following formulas.

$$Recall = \frac{TP}{(TP + FN)} \quad (1)$$

$$False\ Positive\ Rate = \frac{FP}{(FP + TN)} \quad (2)$$

$$False\ Negative\ Rate = \frac{FN}{(FN + TP)} \quad (3)$$

$$False\ Alarm\ Rate = \frac{FP + FN}{(TP + TN + FP + FN)} \quad (4)$$

6. Results and discussion

6.1. Experiment analysis

During the experiment analysis, the model was able to achieve 99.83% accuracy. Fig. 7 shows the confusion matrix obtained from the model training. The DDoS classification recall can be termed as the detection rate or sensitivity indicator of the model. Based on Eq. 1, the model managed to achieve a

99.84% detection rate. The false-positive rate can be specified as Eq. 2 and the model managed to achieve a false-positive rate of 0.18%. Eq. 3 specified the false-negative rate and the model managed to achieve a false-negative rate of 0.17%. Eq. 4 specifies the false alarm rate and the model managed to achieve an overall false alarm rate of 0.18%.

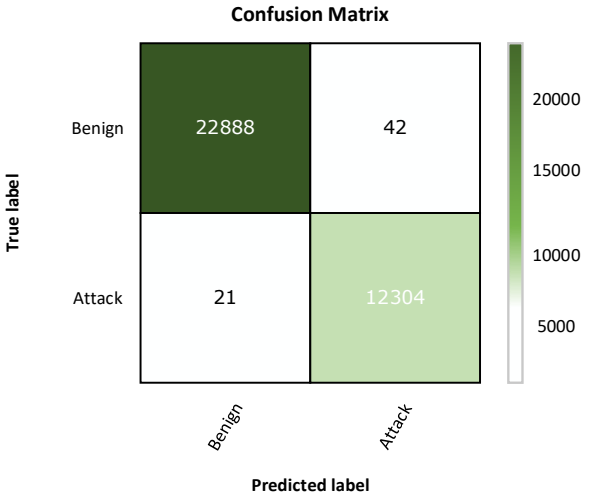

Fig. 7: Confusion matrix from model training

6.2. Evaluation with MazeBolt PCAP files

To access the effectiveness of the proposed detection, model the MazeBolt PCAP files were tested by using the model. MazeBolt is a cybersecurity firm that offers the latest different types of application-layer DDoS attack PCAP files under their knowledge base (MazeBolt, 2020). They have provided 24 types of application-layer DDoS attack PCAP files that contain a specific category of application-layer DDoS attack type in each PCAP file.

The traffic information contained in those PCAP files is extracted and tested using the proposed model. The model was able to detect all the different attack types except Apache Benchmark HTTP application layer DDoS attack. Table 5 shows the experiment results.

Detecting of new patters or unseen patterns of application-layer DDoS attack capability of the model is tested by using the GANs power. The GANs are built to generate new application-layer DDoS attack patterns using the existing application layer DDoS patterns in the dataset. The model was able to detect new patterns generated by the GANs.

6.3. Comparison evaluation

For the comparison evaluation, it has selected six experiments that have been done to detect application-layer DDoS attacks from the literature reviews. The selected experiments have used different approaches for the detection. Table 6 shows the details of each experiment study.

There are a couple of studies that have achieved a similar detection rate. Yadav and Subramanian (2016) have achieved a detection rate of 98.99%, but the false-positive rate is 1.27. A similar feat was achieved by Singh and De (2019) with a detection rate of 98.04% but the false-positive rate is unknown from their study. The proposed model has achieved a detection rate of 99.84% while maintaining a false-positive rate of 0.18%. The comparison proved that the model able to achieve a high detection rate while maintaining the low false-positive rate. Even though other studies that are listed in Table 6, not reveal the overall false alarm rate that is an important indication for a detection model the proposed model was able to achieve a 0.18% overall false alarm rate.

Table 5: model experiment with different DDoS attack types

DDoS Attack Types	Number of Traffics in PCAP	Prediction		Prediction%	Time Taken for the Prediction(sec)
		Benign	DDoS Attack		
HTTP PUT Flood	40	0	40	100%	5.185
HTTP Connect Flood	31	0	31	100%	4.051
HTTP DELETE Flood	30	0	30	100%	4.056
HTTP Flood	209	0	209	100%	27.939
HTTP GET Flood	30	0	30	100%	4.212
HTTP POST Flood	46	0	46	100%	6.543
Slowloris Attack	500	0	500	100%	65.621
HTTPS Flood	40	0	40	100%	5.606
Hulk Flood	37	0	37	100%	5.186
HTTP TRACE Flood	40	0	40	100%	5.059
HTTP HEAD Flood	30	0	30	100%	4.104
Apache Benchmark HTTP	56	41	15	27%	8.862
Brobot Attack	207	0	207	100%	27.477
DNS Request Flood	1	0	1	100%	0.258
DNS Response Flood	2	0	2	100%	0.324
Dns Sec Flood	1	0	1	100%	0.224
Dynamic HTTP Flood	140	0	140	100%	17.895
Golden Eye HTTP Flood	188	0	188	100%	25.028
HTTP Options Flood	40	0	40	100%	5.187
HTTP Patch Flood	40	0	40	100%	5.447
HTTPS Flood BE	107	0	107	100%	14.443
IPSEC IKE Flood	120	0	120	100%	15.096
THC-SSL Attack	21	0	21	100%	3.115
Tor's Hammer Attack	465	0	465	100%	63.073
Total Traffic Flow		2421			
Average Percentage		97%			
Average sec per Traffic Flow		0.1338			

Table 6: Comparison evaluation with similar studies

Author	Research Title	Detection Rate	False Positive Rate
Xie and Yu (2006)	A Novel Model for Detecting Application Layer DDoS Attacks	90	1
Liao et al. (2015)	Application layer DDoS attack detection using cluster with a label based on sparse vector decomposition and rhythm matching	78.95	0.14
Ye et al. (2012)	Application layer DDoS detection using clustering analysis	93.16	Unknown
Yadav and Subramanian (2016)	Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder	98.99	1.27
Singh and De (2019)	MLP-GA based algorithm to detect application layer DDoS attack	98.04	Unknown
Ni et al. (2013)	Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis	97.81	2.05
Proposed Model		99.84	0.18

7. Conclusion and Future work

In this paper, an approach to detect application-layer DDoS attacks is proposed by using autoencoder as the feature selection technique and deep neural networks as the attack classifier. The proposed model provides a detection rate of 99.84% while maintaining a false positive rate of 0.18% and a false-negative rate of 0.17%.

Based on the business impact of the problem both false positive and false negative rates are important. False-negative will allow the attackers to reach the intended endpoint which will inversely impact the business availability. The reduction of availability will impact the business's bottom and the top lines. False-positive will block the legitimate users from being able to obtain the service they looking for which impacts the brand quality of the business while reducing the bottom and the top lines. Hence any type of false alarm has its impact on the business. The model managed to achieve an overall false alarm rate low as 0.18%.

The model is capable of detecting most of the latest application layer DDoS attack types available. The new attacking pattern generated by GANs using the existing attack patterns is also detected by the proposed model.

The model uses a PCAP file to extract packet information. But in the future, techniques like NetFlow, J-Flow, or s-Flow can be used as mentioned techniques provide faster performances to extract packet information when it comes to live traffic monitoring. Since the model has a higher detection rate with a low false alarm rate, can be applied in the actual network for application-layer DDoS detection.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Alkasassbeh M, Al-Naymat G, Hassanat A, and Almseidin M (2016). Detecting distributed denial of service attacks using data mining techniques. International Journal of Advanced Computer Science and Applications, 7(1): 436-445. https://doi.org/10.14569/IJACSA.2016.070159

Asad M, Asim M, Javed T, Beg MO, Mujtaba H, and Abbas S (2020). Deepdetect: Detection of distributed denial of service attacks using deep learning. The Computer Journal, 63(7): 983-994. https://doi.org/10.1093/comjnl/bxz064

Bediako PK (2017). Long short-term memory recurrent neural network for detecting DDoS flooding attacks within TensorFlow Implementation framework. Available online at: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1160966&dswid=8339

Behal S and Kumar K (2016). Trends in validation of DDoS research. Procedia Computer Science, 85: 7-15. https://doi.org/10.1016/j.procs.2016.05.170

Chio C and Freeman D (2018). Machine learning and security. O'Reilly Media, Inc., Sebastopol, USA.

Cisco (2018). Cisco annual internet report. Available online at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Cisco (2018). Cisco annual internet report. Available online at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Dertat A (2017). Applied deep learning-part 3: Autoencoders. Available online at: https://towardsdatascience.com/applied-deep-learning-part-3-autoencoders-1c083af4d798

Douligeris C and Mitrokotsa A (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. Computer Networks, 44(5): 643-666. https://doi.org/10.1016/j.comnet.2003.10.003

Filho LFSD, Silveira FA, de Medeiros BJA, Vargas-Solar G, and Silveira LF (2019). Smart detection: An online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks, 2019: 1574749. https://doi.org/10.1155/2019/1574749

Gupta A (2018). Distributed denial of service attack detection using a machine learning approach. Available online at: https://prism.ucalgary.ca/handle/1880/107615

Imamverdiyev Y and Abdullayeva F (2018). Deep learning method for denial of service attack detection based on restricted Boltzmann machine. Big Data, 6(2): 159-169. https://doi.org/10.1089/big.2018.0023 **PMid:29924649**

Ippolito PP (2019). Feature extraction techniques. Available online at: https://towardsdatascience.com/feature-extraction-techniques-d619b56e31be

Jazi HH, Gonzalez H, Stakhanova N, and Ghorbani AA (2017). Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. Computer Networks, 121: 25-36. https://doi.org/10.1016/j.comnet.2017.03.018

Jordan J (2018). Introduction to autoencoders. Available online at: https://www.jeremyjordan.me/autoencoders/

Kale M and Choudhari DM (2014). DDOS attack detection based on an ensemble of neural classifier. International Journal of Computer Science and Network Security, 14(7): 122-129.

Kim M (2019). Supervised learning-based DDoS attacks detection: Tuning hyperparameters. Electronics and Telecommunications Research Institute (ETRI) Journal, 41(5): 560-573. https://doi.org/10.4218/etrij.2019-0156

Liao Q, Li H, Kang S, and Liu C (2015). Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching. Security and Communication Networks, 8(17): 3111-3120. https://doi.org/10.1002/sec.1236

MazeBolt (2020). MazeBolt knowledge base. Available online at: https://kb.mazebolt.com/

Mhamdi L, McLernon D, El-moussa F, Zaidi SAR, Ghogho M, and Tang T (2020). A deep learning approach combining autoencoder with one-class SVM for DDoS attack detection in SDNs. In the IEEE Eighth International Conference on Communications and Networking (ComNet), IEEE, Hammamet, Tunisia: 1-6. https://doi.org/10.1109/ComNet47917.2020.9306073

Nash C (2019). Create data from random noise with generative adversarial networks. Available online at: https://www.toptal.com/machinelearning/generative-adversarial-networks

Ni T, Gu X, Wang H, and Li Y (2013). Real-time detection of application-layer DDoS attack using time series analysis. Journal of Control Science and Engineering. https://doi.org/10.1155/2013/821315

Noh S, Lee C, Choi K, and Jung G (2003). Detecting distributed denial of service (ddos) attacks through inductive learning. In the International Conference on Intelligent Data Engineering and Automated Learning, Springer, Hong Kong, China: 286-295. https://doi.org/10.1007/978-3-540-45080-1_38

Norton (2020). What is a DDoS attack? Available online at: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

Paliwal S and Gupta R (2012). Denial-of-service, probing and remote to user (R2L) attack detection using genetic algorithm. International Journal of Computer Applications, 60(19): 57-62.

Petters J (2019). What is a distributed denial of service (DDoS) attack? Available online at: https://www.varonis.com/blog/what-is-a-ddos-attack/

Phan TV, Gias TR, Islam ST, Huong TT, Thanh, NH, and Bauschert T (2019). Q-MIND: Defeating stealthy DoS attacks in SDN with a machine-learning based defense framework. In the IEEE Global Communications Conference, IEEE, Waikoloa, USA: 1-6. https://doi.org/10.1109/GLOBECOM38437.2019.9013585

Revathi S and Malathi A (2014). Detecting denial of service attack using principal component analysis with random forest classifier. International Journal of Computational Science and Engineering and Technology, 5: 248-252.

Rupak RB (2020). LSTM-AutoEncoders. Available online at: https://medium.datadriveninvestor.com/lstm-autoencoders-f4fdd00cb32c

Sharafaldin I, Lashkari AH, Hakak S, and Ghorbani AA (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In the International Carnahan Conference on Security Technology, IEEE, Chennai, India: 1-8. https://doi.org/10.1109/CCST.2019.8888419

Singh KJ and De T (2020). Efficient classification of DDoS attacks using an ensemble feature selection algorithm. Journal of Intelligent Systems, 29(1): 71-83. https://doi.org/10.1515/jisys-2017-0472

Wankhede S and Kshirsagar D (2018). DoS attack detection using machine learning and neural network. In the Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE, Pune, India: 1-5. https://doi.org/10.1109/ICCUBEA.2018.8697702

Xie Y and Yu SZ (2006). A novel model for detecting application layer DDoS attacks. In the First international multi-symposiums on computer and computational sciences, IEEE, Hangzhou, China, 2: 56-63. https://doi.org/10.1109/IMSCCS.2006.159

Yadav S and Subramanian S (2016). Detection of application layer DDoS attack by feature learning using Stacked AutoEncoder. In the international conference on computational techniques in information and communication technologies, IEEE, New Delhi, India: 361-366. https://doi.org/10.1109/ICCTICT.2016.7514608

Ye C, Zheng K, and She C (2012). Application layer DDoS detection using clustering analysis. In the 2nd International Conference on Computer Science and Network Technology, IEEE, Changchun, China: 1038-1041. https://doi.org/10.1109/ICCSNT.2012.6526103 **PMid:22897662 PMCid:PMC3547140**