Journal of Information Systems Engineering and Management
2025, 10(20s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Advancing DDoS Attack Detection Using Machine Learning Strategies

Jyotsna Nanajkar[1] and Sudhir B Lande[2]

[1]PhD Scholar, Electronics and Telecommunication Dept., SVPM's COE, Malegaon, India

[2]Professor, Electronics and Telecommunication Dept., VPKBIET, Baramati, India

njyo08@gmail.com1, sudhir.lande@vpkbiet.org2

ARTICLE INFO

Received: 22 Dec 2024

Revised: 27 Jan 2025

Accepted: 15 Feb 2025

ABSTRACT

A vast amount of data is generated and saved on the cloud and other virtual storage systems as a result of the advancement of technologies like networking, cloud computing, and the Internet of Things (IoT) Massive volumes of data are sent and received over public or private networks, and mobile networks, Internet of Things networks, and other physical networks are essential for storing, sending, and analyzing that data. However, as a result of this rapid advancement in networking, cyberattacks have been observed on these networks, posing serious problems to the data security of these networks. Distributed Denial of Service (DDoS) attacks are the most common cyberattacks seen on any network, according to a recent survey. A network is inundated with DDoS attacks, which prevents the network from offering services to the authorized users. A Convolutional Neural Network-Visual Geometry Group (CNN-VGG) model developed in this study identifies DDoS attacks on any network. In proposed approach, CIC-IDS2017 (Intrusion Detection System) dataset is transformed into images, the model is trained and validated using these images. The model's performance is evaluated using measures like F1 Score, Accuracy, Precision, and Recall. The VGG model has proved a 92% accuracy rate in detecting DDoS attacks.

Keywords: IoT, DDoS Attack, CNN, VGG, ResNet, CICIDS2017.

INTRODUCTION

As networking technologies evolve, an increasing amount of data is transmitted across open and unprotected networks. This data is at risk of being intercepted and compromised through various forms of cyberattacks, potentially exposing sensitive personal or organizational information. These attacks can lead to data manipulation, theft, or destruction, and they can be carried out manually or automatically. Recent statistics show a dramatic rise in cyberattacks, with incidents spiking by 125% in 2023 compared to the previous years. A significant surge in DDoS attacks is observed over recent years, with no signs of this trend slowing down. In fact, projections suggest that DDoS attacks will have increased by over 300% in 2024 alone. This growing threat poses significant risks to both businesses and individuals, as these attacks can cause severe disruptions to websites and online services. To combat this, several strategies and tools are being developed to detect and mitigate DDoS attacks on the network level [1].

1.1 DDoS Attack

It is a malevolent endeavor that aims to prevent a server, service, or network from functioning normally by overloading the target or the infrastructure around it with excessive Internet traffic. This flood of traffic can include a variety of data types, such as requests for connections or information, which exhausts the target's resources and keeps authorized users from accessing it [2]. DDoS assaults can be carried out via a botnet, which is a network of compromised machines. This allows the attacker to manage and plan the attack simultaneously from multiple places. The targeted firm or person may suffer major financial losses, outages, and harm to their reputation as a result of these attacks [3].

1.2 Machine Learning Strategies

Research on DDoS attacks is a hot area, and there are a number of techniques for identifying and stopping DDoS attacks. Creating an intrusion detection system or applying artificial intelligence techniques could aid in identifying the attack. For identifying DDoS attacks, a number of methods and algorithms are widely utilized, including CNN, Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN), ResNet (Residual Networks), VGG and many more.

1.2.1 CNN

For image recognition and classification applications, convolutional neural networks, or CNNs, are a popular kind of deep learning technique. Convolution, pooling, and completely linked are the three layers that comprise the CNN

model. images using a series of pooling, convolutional, and fully connected layers. In order to capture the spatial hierarchies of features such as edges, textures, and shapes, the convolutional layers apply filters to the input image. Subsequently, pooling layers down sample the feature maps, reducing their dimensionality without erasing valuable information [4] Last but not least, fully linked layers make predictions about things like which objects or patterns are in the image using the information that has been collected.

1.2.2 ResNet

A kind of deep learning architecture called ResNet was created to overcome the difficulties associated with training extremely deep neural networks. ResNet, which was first presented by Microsoft Research, employs the idea of residual learning, in which one or more layers are skipped during training by adding shortcut connections. This lessens the vanishing gradient issue, making it possible to train deeper models more effectively and find complex patterns in big datasets like those used in DDoS attack detection.

1.2.3 VGG

It is known for its deep convolutional neural network design, VGG has significantly improved computer vision tasks. The University of Oxford created the VGG16 model, which is renowned for being straightforward and efficient. Three fully connected layers and thirteen convolutional layers make up its sixteen layers. VGG16 employs hierarchically stacked tiny 3x3 convolutional filters. VGG19 is one more in the series.

1.2.4 LSTM

One kind of RNN that makes use of specialized units known as memory cells is termed LSTM. The capacity of LSTM to preserve long-term dependencies in the data is its primary benefit over conventional RNNs. In time-series data, where past occurrences can impact future ones, its ability to remember information over extended periods of time is especially helpful.

RELATED WORK

DDoS attacks are cyber-attacks that are used to flood a system so that it cannot provide services to its legitimate uses. There are several researches made on spotting DDoS attacks using machine learning and deep learning techniques. This section provides a\ detailed survey of several pieces of research done on detecting and preventing DDoS and other cyber-attacks.

Gebresilassie, Joseph Rafferty, Liming Chen, Zhan Cui, and Mamun Abu-Tair [5], proposed a model that addresses a number of drawbacks in intriguing solutions of transfer learning and CNN based IDS for DDoS attack detection. The suggested work creates real-time attack data as part of a revolutionary data pre-processing procedure. This research compares the accuracy of three models -VGG, RestNet, and Inception V3 - in detecting DDoS attacks, with a final result of 99.36%.

Abdullah I. A. Alzahrani, Manel Ayadi, Mashael M. Asiri, Amal Al-Rasheed, and Amel Ksibi [6],[23] proposed a multi-stage architecture made up of two modified VGG-19 models. The initial goal of the model is to determine if the input file is dangerous or not. If the file is found to be malicious by the first model, the second purpose of the model is to determine the type of malware. On 80% of the data, the two models were trained, and on the remaining 20%, they were tested. On the testing set, the VGG-19 model's first stage achieved 99% accuracy. With an accuracy of 98.2% on the testing set, the second step, which used the VGG-19 model, was in charge of identifying the type of malware - five distinct types were present in the dataset.

Lan Liu, Pengcheng Wang, Jun Lin, and Langzhou Liu [7] suggest that malicious attacks can conceal themselves in large amounts of normal data, creating a large amount of imbalanced data that is difficult to identify, making it challenging for the Network Intrusion Detection system (NIDS) to achieve better accuracy and results. By applying the Difficult Set Sampling Technique (DSSTE) algorithm, imbalance issues are addressed. We perform experiments using the more recent and extensive intrusion dataset CSE-CIC-IDS2018, as well as the traditional intrusion dataset NSL-KDD, to validate the suggested technique. We employ the Random Forest (RF), Support Vector Machine (SVM), XGBoost, Long and Short-Term Memory classical classification models.

Meenakshi Mittal, Krishan Kumar, and Sunny Behal [8] examined the SLR of five distinct research areas on DDoS attack detection. DL techniques, advantages and disadvantages of current DL techniques Transfer learning evaluated in detail. The research gap also includes hyper-parameter, system performance, and metrics.

Xiaoyong Yuan, Chuanhuang Li, and Xiaolin Li of the Large-scale Intelligent Systems Laboratory, University of Florida Zhejiang Gongshang University [9] describe a DDoS Attack Detection Approach called Deep Defense that automatically extracts high-level features from low-level and provides a solid representation. In order to extract the intricate pattern from the flow of network traffic operations, they created a RNN model. This paper's primary goal is to improve the model's performance using older machine learning models, where error rates were decreased from 7.5% to 2.1%.

As proposed by Naeem Firdous Syed, Zubair Baig, Ahmed Ibrahim, and Craig Valli [10] in their paper, Message Queuing Telemetry Transport (MQTT) IoT protocol datasets utilized, and the alleged sophistication of recent works in this field. Deep learning techniques used to conclude detection accuracy of 99%.

Mengmeng Ge, Naeem Syed, Zubair Baig, Gideon Teo, and Antonio Robles-Kelly [11] in the article provide a unique intrusion detection strategy for IoT networks that uses deep learning concepts to classify traffic flow. To classify data into binary and multiclass categories, they used feedforward neural networks. Features extraction, feature preprocessing, training, and classification are the four primary stages of the system they utilized. DDoS, DoS, reconnaissance, information theft, and regular traffic are the five types of assaults used in this paper. With regard to binary classification accuracy, strong recall and precision values (all over 0.99), and a high F1 score above 0.999. Similarly for multiclass classification, 0.99 accuracy for detecting normal traffic, for DDOS and DOS and Reconnaissance 0.98 and Information theft attack 0.89 accuracy.

Table 1 provides a detailed survey of different research methods made on spotting and preventing DDoS attacks on different types of datasets.

Table 1: Comparison of Different Methodologies

Ref	Algorithm	Datasets	Accuracy (%)
12	GA with RF	UNSW-NB15	87.61
	GA with RF		77.64
13	KNN	R2L and U2R	85.21
	RF	Probe and DoS Attacks	87.78
	DT	NSL-KDD	-
14	CNN	UNSW Canberra	91.27
	MLP		79.01
15	DNN	NSL-KDD	86.00
16	DNN	UNSW-NB15	88.00
17	DNN- LSTM	KDD99	85.65
18	CNN- LSTM	NSL-KDD	81.33
19	CNN-LSTM	NSL-KDD	83.31

METHODOLOGY

The most cutting-edge technologies utilized in many different sectors nowadays are AI and ML. Numerous studies have been conducted on the use of AI and ML approaches in the development of IDS. This section outlines a thorough process for identifying DDoS assaults.

3.1 Selection of Dataset and features

Quality of the data directly affects accuracy of the machine learning models and its performance. Datasets are crucial for obtaining high accuracy. DDoS assaults are detected using a variety of datasets. The goal of datasets is to supply crucial characteristics or factors that aid in the model's precise attack detection [20]. The CIC-IDS 17 dataset [22] is utilized for both training and validating the proposed VGG model. A brilliant tool created to increase the usefulness of intrusion detection and prevention systems is the CIC-IDS 2017 dataset. By offering a wide range of real-world benign and malicious network traffic, including the most recent attacks, it overcomes the limitations of earlier datasets. For identifying DDoS assaults, the CIC-IDS 2017 dataset offers 79 crucial criteria. The dataset provides a realistic testing environment for anomaly-based intrusion detection because it is enhanced with thorough traffic analysis and tagged flows. The features are greatly influenced by the network's type and pattern. The CIC-IDS 2017 dataset, with 79 useful attributes, used in proposed method. Main contributions are pkt length, flag count, flow etc.

3.2 Data Preprocessing

The complex process of turning comma-separated values (CSV), a format that is both ubiquitous and modest, into rich, educational graphics that go beyond the confines of spreadsheets and tables is explored in "Transforming CSV Data into Visual Imagery". Data preprocessing has been performed before image processing. It involves all necessary steps to take care of all +- *inf* and null values appearing in dataset, removal of commas or other special character. Label encoding was used to convert categorical data in numerical values. This article offers a thorough method for turning data from CSV files into pictures. Every row in the CSV file is transformed into a single, 800x600 pixel image in this conversion step. Image conversion of data is performed in Python after importing necessary libraries and loading the required dataset. Row wise, data gets reshaped to a single row matrix and converted to an image.

3.3 Model Formation for DDoS Attack Detection

This section provides a detailed step-by-step implementation of the VGG16 model for spotting DDoS attacks.

3.3.1 VGG16

As shown in fig. 1, VGG-16, a convolutional neural network model, stands out for its depth and uniform architecture, which has been influential in the field of deep learning for image recognition. With 16 layers, including 13 convolutional layers, VGG-16 employs small, 3x3 convolutional filters, which allow it to capture a wide range of features at different levels of abstraction. This design choice contributes to its ability to perform exceptionally well on large-scale image recognition tasks.[8] Despite the emergence of newer models, VGG-16 remains a popular choice for many computer vision applications due to its simplicity, ease of implementation, and strong performance on various benchmarks. It's architecture has become a standard reference for convolutional networks in the image recognition domain.[23]

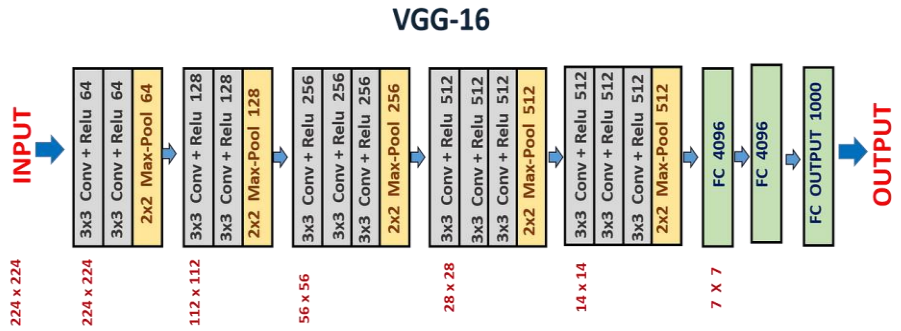

Fig. 1: CNN Model

Table 2: Hyperparameters used in model

Hyper – Parameter	Value
Activation `	Sigmoid, Relu
Optimizer	RMSprop (lr=0.0001)
Loss Function	Binary cross entropy
Metrics	Accuracy
Steps per epoch	453
Epochs	25
Batch size	32

The .csv+ file is transformed into an image dataset in the suggested approach. The matplotlib and NumPy packages in Python are used to complete this task. A separate image is generated for each row. Images formed are of two classes DDoS and Benign (regular traffic). There are almost 14,000 images in total. They are separated into 7000 attacks and 7000 benign images. Use of Google Collab is incorporated to enhance the speed. The model is processed, implemented, and evaluated using essential Python libraries such as sklearn, keras, matplotlib, and tensor flow. Image Data Generator is used to modify the images from TensorFlow and Keras. The VGG16 model is trained using these images and a set of hyperparameters, including batch size, optimizer, activation function, and epoch count is as shown in table 2.

Along with VGG16 model, similar methodology is used for RestNet 50 and CNN models. Results of these models is compared with VGG16 as the proposed work and find the best model with high accuracy.

3.4 Evaluation

Accuracy, Precision, Recall and F1 Score are the parameters used for evaluating the performance of the VGG16 model. Using these metrics model provides four parameters for calculation True Positive (TP), True Negative (TN), False Positive (EP) and False Negative (FN). Based on these values evaluation metrics is calculated [9]. Following are the 4 equations formulas used to calculate evaluation metrics.

Accuracy = (TP+TN)/(TP+TN+FP+FN)

Precision = TP/(TP+FP)

Recall = TP/(TP+FN)

F1-Score = 2*(Precision* Recall)/ (Precision +Recall)

RESULT AND DISCUSSIONS

This section summarizes results of all different methods such as VGG 16, ResNet and CNN employed for intrusion detection improvement. Table 4 provides detailed information on the evaluation metrics used to examine the performance of the proposed model using 3 different algorithms. Parameters studied are accuracy, precision, recall and F1-score. As given in the table 3, and shown in figure 2 proposed VGG16 model exhibits accuracy up to 92% along with 90%, 91%, and 90% precision, recall and F1 score respectively. Figure 3 and 4 show performance for ResNet 50 and CNN method.

Table 3: Evaluation Parameters

Metrics Model	Accuracy	Precision	Recall	F1-Score
VGG16	92	90	91	90
RestNet50	93	89	88	89
CNN	77	85	79	76

Figures 2, 3 and 4 show accuracy graphs captured for CNN VGG 16, ResNet 50 and CNN models respectively.

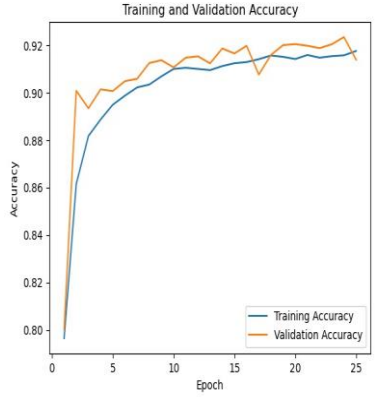

Fig 2. VGG 16 Model

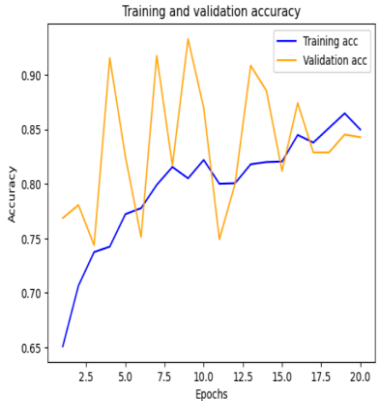

Fig 3. ResNet 50 Model

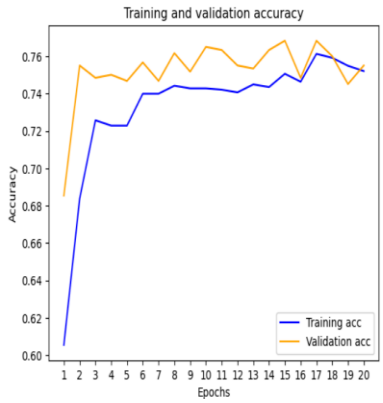

Fig 4. CNN Model

Comparing to the existing research as shown in table 1, results gained in proposed system are better and models exhibits good performance.

CONCLUSION

The rapid expansion of IoT networks has initiated an era where data is the life of communication and technological advancement. However, this progress is not without its perils, as evidenced by the occurrence of DDoS attacks that threaten to undermine the very fabric of our interconnected systems. The research presented herein highlights the vulnerability of IoT networks and works on the efficacy of innovative machine-learning techniques, such as the CNN(VGG16) model, in combating these cyber threats. Figures received as a result can be improved by processing more no of images with the help of advanced CPU and GPU combinations. In this paper a comparative study was carried out between different CNN models to detect DDoS attack accuracy in which VGG 16 outperformed. A hybrid experimentation approach may prove it better and result into big milestone in future.

REFERENCES

[1] Alahmadi, A.A.; Aljabri, M.; Alhaidari, F.; Alharthi, D.J.; Rayani, G.E.; Marghalani, L.A.; Alotaibi, O.B.; Bajandouh, S.A. "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions" Electronics 2023, 12, 3103. https://doi.org/10.3390/electronics12143103

[2] V. Deepa, K. M. Sudar and P. Deepalakshmi, "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques" 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2018, pp. 299-303, doi: 10.1109/ICSSIT.2018.8748836.

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

[4] S. Z. Lin, Y. Shi and Z. Xue, "Character-Level Intrusion Detection Based On Convolutional Neural Networks" 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 2018, pp. 1-8, doi: 10.1109/IJCNN.2018.8488987.

[5] Gebresilassie, S.K.; Rafferty, J.; Chen, L.; Cui, Z.; Abu-Tair, M. "Transfer and CNN-Based De-Authentication (Disassociation) DoS Attack Detection in IoT Wi-Fi Networks" Electronics 2023, 12, 3731. https://doi.org/10.3390/electronics12173731

[6] Alzahrani AIA, Ayadi M, Asiri MM, Al-Rasheed A, Ksibi A. "Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques" Electronics. 2022; 11(22):3665. https://doi.org/10.3390/electronics11223665

[7] L. Liu, P. Wang, J. Lin and L. Liu, "Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning" in IEEE Access, vol. 9, pp. 7550-7563, 2021, doi: 10.1109/ACCESS.2020.3048198

[8] Mittal, M., Kumar, K. & Behal, S. "Deep learning approaches for detecting DDoS attacks: A systematic review" Soft Comput 27, 13039–13075 (2023). https://doi.org/10.1007/s00500-021-06608-1.

[9] X. Yuan, C. Li and X. Li, "Deep Defense: Identifying DDoS Attack via Deep Learning" 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, China, 2017, pp. 1-8, doi: 10.1109/SMARTCOMP.2017.7946998.

[10] Naeem Firdous Syed, Zubair Baig, Ahmed Ibrahim, and Craig "Denial of service attack detection through machine learning for the IoT" Journal of Information and Telecommunication, 4(4), 482-503. https://doi.org/10.1080/ 24751839.2020.1767484

[11] Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly "Deep Learning-Based Intrusion Detection For Iot Networks" 2019 IEEE 24th Pacific Rim International Symposium On Dependable Computing (PRDC) 2473-3105/19/$31.00 ©2019 IEEE DOI 10.1109/PRDC47002.2019.00056.

[12] Sydney Mambwe Kasongo, "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms" IEEE Access, vol. 9, pp. 113199 -113212, Aug 2021

[13] Poulmanogo Illy, Georges Kaddoum, Kuljeet Kaur, Sahil Garg "ML-Based IDPS Enhancement With Complementary Features for Home IoT Networks" IEEE Transactions On Network And Service Management, vol. 19, no. 2, pp. 772-783, June 2022

[14] Bambang Susilo and Riri Fitri Sari "Intrusion Detection in IoT Networks Using Deep Learning Algorithm" Information 2020, 11, 279 © MDPI

[15] J. Jose and D. V. Jose, "Performance analysis of deep learning algorithms for intrusion detection in IoT," in 2021 International Conference on Communication, Control and Information Sciences (ICCISc), Jun. 2021, pp. 1–6, doi: 10.1109/ICCISc52257.2021.9484979

[16] H. Dhillon and A. Haque, "Towards network traffic monitoring using deep transfer learning," in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Dec. 2020, pp. 1089–1096, doi: 10.1109/TrustCom50675.2020.00144

[17] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," Journal of Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00448-4.

[18] Y. Li et al., "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," Measurement, vol. 154, Mar. 2020, doi: 10.1016/j.measurement.2019.107450

[19] X. Zhang, J. Ran, and J. Mi, “An intrusion detection system based on convolutional neural network for imbalanced network traffic,” in 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Oct. 2019, pp. 456–460, doi: 10.1109/ICCSNT47585.2019.8962490

[20] Xavier Larriva-Novo, Víctor A. Villagrá, Mario Vega-Barbas, Diego Rivera And Mario Sanz Rodrigo “An Iot-Focused Intrusion Detection System Approach Based On Preprocessing Characterization For Cybersecurity Datasets” Sensors 2021, 21, 656

[21] Maltare, N. N., Sharma, D. & Patel, S. (2023). An Exploration and Prediction of Rainfall and Groundwater Level for the District of Banaskantha, Gujrat, India. International Journal of Environmental Sciences, 9(1), 1-17. https://www.theaspd.com/resources/v9-1-1-Nilesh%20N.%20Maltare.pdf

[22] Https://www.unb.ca/cic/datasets/ids-2017.html Canadian Institute for Cybersecurity

[23] Geeksforgeeks.com https://www.geeksforgeeks.org/vgg-16-cnn-model