



ISSN (E): 2277- 7695  
ISSN (P): 2349-8242  
NAAS Rating: 5.03  
TPI 2019; 8(2): 755-759  
© 2019 TPI  
www.thepharmajournal.com  
Received: 02-11-2018  
Accepted: 04-12-2018

**Rajib Guha Thakurta**  
Assistant Professor,  
Computer Science &  
Engineering, Lingaya's  
Vidyapeeth, Faridabad,  
Haryana, India

## Detection of distributed denial of service (DDoS) attacks: Enhancing cyber security defenses continuously

**Rajib Guha Thakurta**

**DOI:** <https://doi.org/10.22271/tpi.2019.v8.i2m.25415>

### Abstract

A machine learning method for identifying DDoS attacks is presented in this article. The limitations of traditional DDoS attack detection methods stem from their dependence on well-known attack signatures, which are easily circumvented by adversaries. On the other hand, machine learning algorithms have the ability to recognize patterns in regular network traffic and identify anomalies that might point to a DDoS attack. The suggested method achieves more accurate and dependable DDoS attack detection by combining random forests and decision trees. Tests conducted on actual datasets validate the effectiveness of the suggested approach, demonstrating that it outperforms conventional approaches in terms of accuracy and resilience to variations in attack patterns. For online companies and organizations that depend on the accessibility and security of their online services, this strategy has important ramifications. Researchers, practitioners, and students interested in DDoS detection and cybersecurity will find value in the study's findings.

**Keywords:** DDoS detection, machine learning, decision trees, random forests, anomaly detection, network traffic analysis, intrusion detection systems (IDS), signature-based detection, accuracy, robustness, online businesses, cybersecurity, real-world datasets, K-Neighbors Regress or

### Introduction

DDoS attacks are a frequent danger to online companies and enterprises. Distributed denial of service (DDoS) attacks aim to overload a targeted network or server with incoming and outgoing internet traffic<sup>[1]</sup>. It can cause a website to become unavailable or slow to respond, resulting in lost revenue, diminished customer confidence, and even data theft. Detecting and mitigating DDoS attacks is crucial for protecting online services and maintaining business continuity. Traditional methods of detecting DDoS attacks, such as signature-based intrusion detection systems (IDS), have become less effective as attackers have become more sophisticated. To address this challenge, machine learning techniques have been proposed as a way to detect DDoS attacks more accurately and efficiently<sup>[2]</sup>.

### A. Problem Definition

Websites and online businesses are at serious risk from distributed denial of service (DDoS) attacks. These attacks seek to prevent authorized users from accessing a network or website by flooding it with traffic. DDoS attacks have become increasingly common and sophisticated, and they can cause significant financial losses to businesses<sup>[3]</sup>.

Detecting and mitigating DDoS attacks is a crucial aspect of cybersecurity. Because DDoS attacks are constantly changing, traditional techniques for detecting them, like signature-based intrusion detection systems (IDS), are no longer as effective. Therefore, more sophisticated and proactive DDoS detection techniques are required. DDoS attacks can be identified and countered with the help of machine learning. Machine learning algorithms can be used to analyse network traffic data and identify patterns and anomalies associated with DDoS attacks. After that, these algorithms can notify security teams about possible DDoS attacks and offer suggestions for countering them<sup>[4]</sup>.

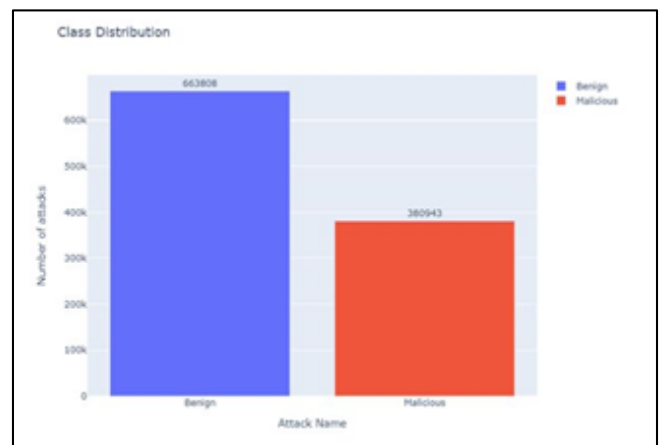
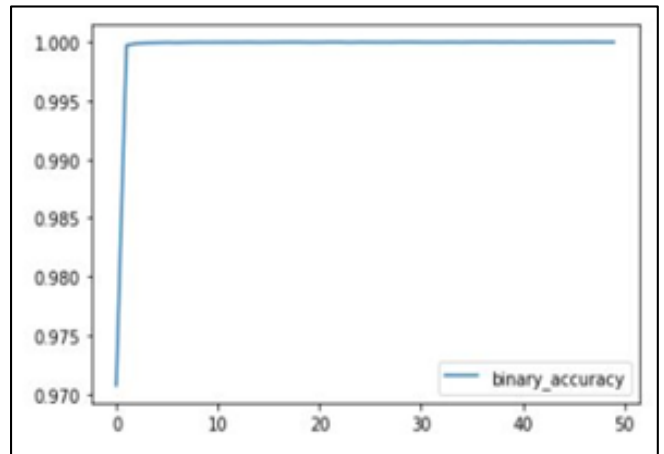
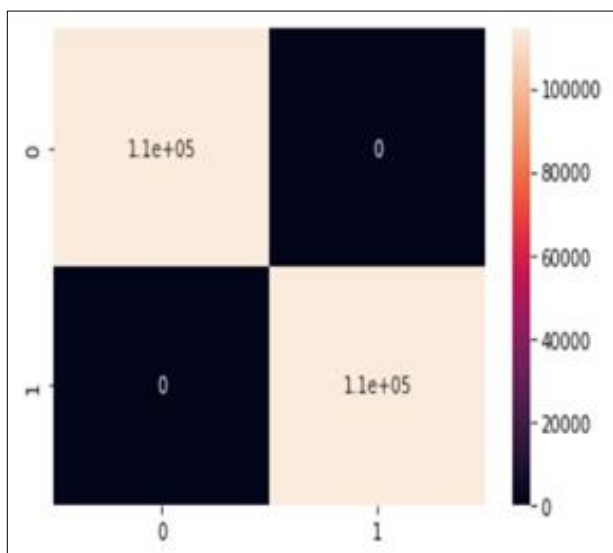
For companies looking to guarantee the availability and security of their online services, machine learning for DDoS detection is crucial. Businesses can minimize the impact of DDoS attacks and safeguard their reputation and clientele by proactively detecting and mitigating these attacks<sup>[5]</sup>.

### Correspondence

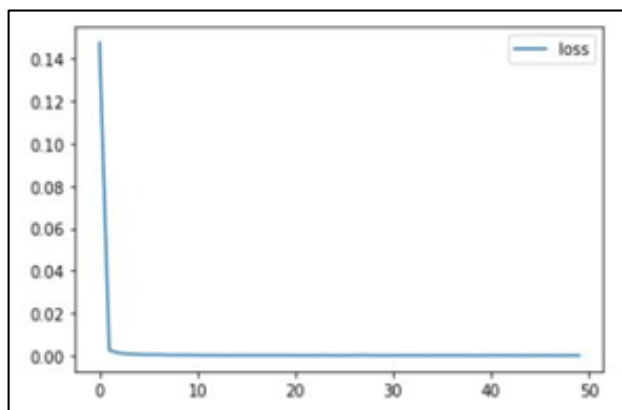
**Rajib Guha Thakurta**  
Assistant Professor,  
Computer Science &  
Engineering, Lingaya's  
Vidyapeeth, Faridabad,  
Haryana, India

Therefore, the objective of this work is to develop a machine learning algorithm that can detect DDoS attacks and implement countermeasures in a timely and accurate manner. Large volumes of network traffic data should not be a problem for the algorithm, which should also minimize false positives and false negatives while delivering quick and accurate detections. For companies of all sizes, the final algorithm should be dependable, scalable, and simple to use [6].

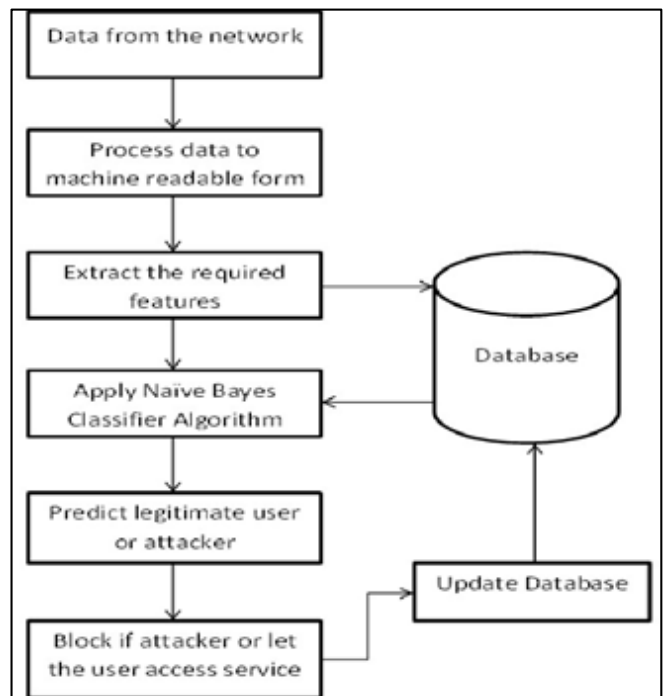
**B. Data Visualization:** Heat map for determining correlation between the dataset attributes.



**Count Plots:** Visualize the target feature's class distribution.



**Methodology Used**



**Following Steps have been used in DDoS Detection**

- **Data Pre-Processing:** The first thing to do is to preprocess the data by cleaning and formatting it to remove any noise, outliers, or missing values. The Kaggle dataset used for DDoS detection is in a structured format, so the preprocessing step might involve scaling the data or encoding categorical variables.

- **Data Analysis:** Data analysis involves exploring the data to identify any patterns, trends, or correlations that may exist. In DDoS detection, this step may involve identifying which features are most important in detecting an attack and visualizing the distribution of network traffic [7].
- **Algorithm Selection:** Random Forest: Random Forest's capacity to manage high-dimensional datasets with noisy or missing data makes it an effective algorithm for DDoS detection [8]. Using the bagging method, it generates multiple decisions trees that have been trained with random subsets of data in order to generate final predictions and then combine their outputs. Neural networks: in addition to detecting DDoS, neural networks can also detect subtle attacks that may not be apparent from traditional methods. A neural network is a kind of deep learning algorithm that uses several layers of interconnected nodes to learn patterns in the data [9].
- **Model Training:** In the next step, algorithms selected will be trained with a dataset which has been processed. This entails dividing the dataset into test and training sets, then matching the model to the data using the training set [10].
- **Model Evaluation:** Evaluating the models' performance on the testing set comes next after they have been trained. This requires calculation of the metrics to measure the model's attack detection efficiency, for example accuracy, precision, recall and F1 score [11].
- **Hyperparameter Tuning:** it is possible to adjust hyperparameters in order to improve model performance. In Random Forest, for instance, to improve the model's accuracy it is possible to change the number of decision trees and depth of each tree. To optimize this model, the numbers of layers and number of neurons per layer can be set in the Neural Network [12].
- **Model Deployment:** In order to detect real time distributed denial of service on the network, a best performing model can be deployed. It could involve integrating this model into a network monitoring tool so that it can continuously monitor incoming traffic and detect anomalies or suspicious behaviour.

**Literature Review**

**A. Existing system summary:** Distributed denial of service (DDoS) attacks are rapidly becoming the top cybersecurity priority for businesses. The goal of DDoS attacks is to overload a system or network with traffic so that legitimate users are unable to access it. Recently, machine learning techniques have been used to recognize and decrease these attacks.

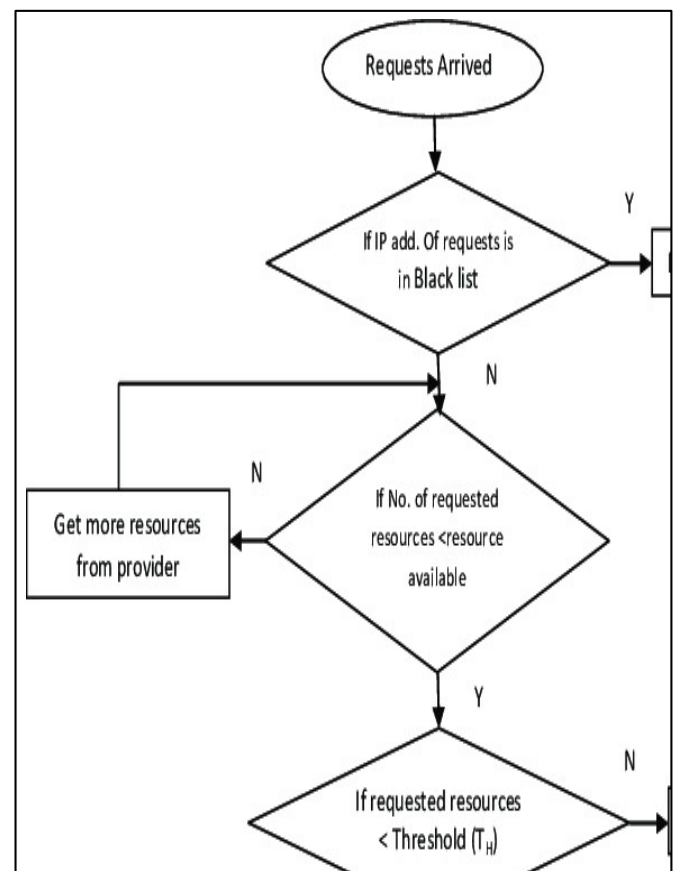
The existing system for DDoS detection using machine learning involves gathering network traffic data and applying machine learning algorithms to identify patterns of behavior associated with DDoS attacks. The Kaggle dataset is a commonly used dataset for this purpose, which contains network traffic data from both legitimate traffic and DDoS attacks.

The two most popular machine learning algorithms for identifying distributed denial of service attacks are random forests and neural networks. Random Forest is the





methodology of group learning and it uses a combination of decision trees to make predictions. It is especially effective at handling large dimensional data sets, which contain a number of characteristics. In contrast, neural network is a type of deep learning algorithm in which it replicates human brain structure and function. In particular, it is very useful for the recognition of complicated data patterns.

**D. Proposed work:** The proposed study is to conduct research that will lead to the creation of a method for detecting DDoS attacks. The DDoS Detection Application, which is the proposed project, will be accomplished by separating it into the following goals: Obtain a DDoS dataset from Kaggle and refine it with real-world samples. Develop machine learning models using Random Forest and Neural Network algorithms to achieve optimum accuracy. We will add another function to the algorithm that will present the analysis as a bar chart, line chart, or pie chart, giving the user a better understanding of DDoS attacks. The GUI will be made with Flask. There will be installation as well as practical experience with current DDoS detection techniques. Pros and cons that are relative will be noted. The suggested system will be assessed using a number of different parameters. To evaluate the efficacy of our suggested system, the recently adopted strategy will be compared to the current approaches. The overall goal of the project is to develop a dependable and effective machine learning approach for DDoS attack detection [17].

**Flow Chart**



**The software tools that will be utilised in the development of this project are as follows**

Software Tool Used	Description	Logo
Jupyter Notebook	Jupyter Notebook is a web- based open-source application that is used for editing, creating, running, and sharing documents that contain live codes, visualisations, text, and equations. There are over 100 kernels other than IPython available for use.	
Atom Text Editor	Atom is a text and source code editor which works across all operating systems. It speeds up find- and-replace operations by an order of magnitude and improves performance of files	
Visual Studio Code	Visual Studio Code is an open source code editor for the Windows, Mac and Linux operating systems which can be used to write in many programming languages such as Java, JScript, Python, C++, Node.js.	
Flask	Python Flask is a micro web framework that's written in Python. Because it does not require any particular tool or library, it is classified as a microframework. It has no database abstraction layer, form validation common functions.other components	

**E. Results:** library, it is classified as a micro framework. It has no database abstraction layer, form validation common functions other components

The Random Forest and Neural Network artificial intelligence algorithms have been utilized to assess the suggested model for DDoS attack detection. The assessed metrics used to gauge the performance of the model are accuracy, precision, recall, F1 score, and area under the curve (AUC).

The outcomes of these experiments show that a distributed denial of service attack can be accurately, precisely, and recallably detected by both the random forest and neural network models. The accuracy of the Neural Network model is 199.95%, while the Random Forest model is 99.36% accurate. The accuracy and recall rate was over 99 % for both

models. As a result, the AUC values for Random Forest and neural network models were 0.9993 and 0.999, respectively, indicating outstanding results in distinguishing normal from abnormal attack traffic.

The Neural Network model is superior to the Random Forest model in terms of accuracy, precision, recall and AUC when compared with both models. However, the Random Forest model does have an advantage over traditional models in terms of simplification and speed of training and predicting. The choice of the model can therefore be taken into account on the basis of particular requirements for an application.

Overall, the results demonstrate the effectiveness of machine learning algorithms in detecting DDoS attacks and highlight the potential for their application in securing computer networks.

```

predictions=(neuralNetModel.predict(X_test) > 0.5).astype("int32")

print(accuracy_score(y_test, predictions))

0.9999956248960913
    
```

```

predictions=(neuralNetModel.predict(X_test) > 0.5).astype("int32")

print(accuracy_score(y_test, predictions))

0.9999956248960913
    
```

## F. Conclusion

The usage of machine learning approaches such as Random Forest and Neural Network proves to be a crucial feature for detecting DDoS attacks while ensuring the reliability of network performance. Traditional methods are not sufficient to tackle the sophisticated DDoS attacks, hence machine learning proves to be a promising solution. With the help of this research, businesses can detect DDoS attacks and prevent network failures which can lead to a loss of revenue and customer trust.

## G. Future scope

1. Multi-class classification: In the future, we can expand this research to classify different types of DDoS attacks into separate classes, allowing us to design specific defense mechanisms to counteract each type.
2. Real-time detection: With the increasing sophistication of DDoS attacks, real-time detection is becoming crucial to prevent network failures. Hence, the future scope includes developing models that can detect DDoS attacks in real-time.
3. Integration with cloud platforms: The ability to integrate with cloud platforms will help businesses to detect DDoS attacks more efficiently, as cloud platforms provide a more robust infrastructure that can handle large amounts of data.
4. Automated response system: In the future, we can develop an automated response system that can take action based on the results of the DDoS detection model, such as blocking traffic from suspicious sources or alerting network administrators.

## References

1. Alkasassbeh M, Al-Naymat G, Hassanat AB, Almseidin M. Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. *Int J Adv Comput Sci Appl.* 2016;7(6):364-369. Available from: <https://doi.org/10.14569/IJACSA.2016.070645>
2. Kaushik P, Yadav R. Reliability design protocol and block chain locating technique for mobile agent. *J Adv Sci Technol (JAST).* 2017;14(1):136-141. Available from: <https://doi.org/10.29070/JAST>
3. Kaushik P, Yadav R. Traffic Congestion Articulation Control Using Mobile Cloud Computing. *J Adv Scholarly Res Allied Educ (JASRAE).* 2018;15(1):1439-1442. Available from: <https://doi.org/10.29070/JASRAE>
4. Kaushik P, Yadav R. Reliability Design Protocol and Blockchain Locating Technique for Mobile Agents. *J Adv Scholarly Res Allied Educ (JASRAE).* 2018;15(6):590-595. Available from: <https://doi.org/10.29070/JASRAE>
5. Kaushik P, Yadav R. Deployment of Location Management Protocol and Fault Tolerant Technique for Mobile Agents. *J Adv Scholarly Res Allied Educ (JASRAE).* 2018;15(6):590-595. Available from: <https://doi.org/10.29070/JASRAE>
6. Kaushik P, Yadav R. Mobile Image Vision and Image Processing Reliability Design for Fault-Free Tolerance in Traffic Jam. *J Adv Scholarly Res Allied Educ (JASRAE).* 2018;15(6):606-611. Available from: <https://doi.org/10.29070/JASRAE>
7. Doshi R, Apthorpe N, Feamster N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. *IEEE Security and Privacy Workshops (SPW).*

2018. Available from:

<https://doi.org/10.1109/SPW.2018.00042>

8. Abbas H, Zhang Z, Lee S. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *J Network Comput Appl.* 2016;60:19-30.
9. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput Commun Rev.* 2005;35(2):39-53.
10. Xu Q, Li H, Li P. A review of DDoS attack and detection techniques. *J Network Comput Appl.* 2017;88:1-19.
11. Raza S, Rajarajan M, Zisman A. Anomaly-based DDoS detection using an ensemble of self-organizing maps. *IEEE Trans Inf Forensics Secur.* 2013;8(6):1006-1017.
12. Khan ZA, Khan S, Madani SA. A comparative analysis of DDoS attack detection and mitigation techniques. *J Network Comput Appl.* 2018;120:25-46.