Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 1 January 2023

Research Article

Framework for Monitoring and Detection of DDOS Attacks using ML Algorithms

Batool Mastoi* and Gul Bano

Department of software Engineering, Mehran University of Engineering and Technology, Jamshoro, Sindh, Pakistan

***Corresponding Author:** Batool Mastoi, Department of software Engineering, Mehran University of Engineering and Technology, Jamshoro, Sindh, Pakistan.

Received: December 20, 2022

Published: December 27, 2022

Abstract

DDOS attacks have become a widespread problem on the internet these days. The DDOS attack is a spiteful effort to dislocate the usual traffic of a targeted server, service, or network by crushing the target or its nearby infrastructure with a flood of Internet traffic. Artificial intelligence and Machine learning proved to be efficient in evaluating the performance of the system by using algorithms. The detection of DDOS attacks is a basic problem in machine learning. Due to the advancement of technology i.e. Cloud computing, it is a significantly difficult task to identify DDOS attacks because of computational complexities. This Study proposes a ML framework for detecting, Monitoring and providing prevention techniques for DDOS attacks and compares the performance of four frequently used algorithms (Nave Bayes, Decision Tree, Random Forest, and SVM). The dataset was validated by performing a T-test. OWASP ZAP and Weka Tool have been used for the analysis. 1031 samples were collected. The study found interesting remarks.

Keywords: DDOs Attack; Ml Algorithms; Owsap Zap; Risk

Introduction

Due to the simple operation and high adeptness in web services attacks, Distributed denial of service (DDOS) is becoming a very common as well as critical web service attack. The main player in this life-changing game is the bot master who acts as the attacker and controls several compromised machines called zombies in DDOS, we have named them botnets. The main and important goal of the Bot Master is to form a botnet and affect many systems on the internet with infected zombies/agents. The attacker controls infected systems remotely. DDoS attacks cost a lot of money, time, and reputation and are serious security problems for organizations and individuals, DDOS is not loss of dataor credentials, but the loss of services internet such as email, online websites, online applications, and their performance its main purpose is to damage maximum no of devices and their resources [1]. Therefore, the purpose of this research is to create a framework that can continuously monitor DDOS attacks and apply feasible actions when DDoS attacks are detected. We will be using Machine Learning Techniques (random forest/Decision tree) and according to specific features of DDoS attacks, the affected traffic will be separated from genuine traffic [13,14].

Although various protection mechanisms have been proposed to control DDoS attacks, with the emergence of modern technologies and platforms in the network field, threats and access to the new look and new natureof DDoS are created daily and challenge new technologies [9].

According to Most Recent readings, attackers create about 1 Tbps + DDoS attack from an area of the world having high bandwidth and poor structure and arrangement practices, where the attacker generated raw traffic directly from his comfort zone called HOME. Security over web applications is one of the main parts while sending data over the internet itself risk to protect data over the internet many techniques were discovered. Several ways hackers' attacks the victim's server but attacking through web links is a little bit easier. Due to advancements in technologies, itis easier to steal data from a computer or client machine by using some

software or doing programming for instance Wi-Fi hacking, utilizing CPU or memory, etc. The researchers suggest that invaders can launch various types of DDOS attacks through mobile phones It is also suggested by a researcher that invaders can launch several types of DDoS doses from mobile phone botnets. In one of the attacks, the attacker has the botnet randomize all cellular identifiers by issuing emergency calls frequently. Since there exist legitimate anonymous emergency calls, the network as well as the emergency call centers were not able to block these undesired calls(technically and legally) [10,11].

Artificial intelligence is a field of science that makes machines act like a human. A system, a way of thinking, a way of learning, and a way to solve problems are all included. Thus, an intelligent system was built. In this field, computer science, biology, mathematics, and engineering are combined. Artificial Intelligence (AI) has many applications. AI is used in modern gaming applications. Natural Language Processing is one aspect of AI research. Industrial Robotics is another example [16].

Artificial Intelligence involves Machine Learning. Through it, computers can learn without being unambiguously programmed. There are several Machine Learning algorithms available. It is possibleto select the appropriate Machine Learning algorithm based on the type of problem. By developing computer programs that can react to new data, it can provide a result.

This research study introduces a ML framework for detecting, monitoring, and solving DDOS attack issues for Websites, and based on attacks dataset the performance of Machine learning algorithms (SVM,Decision Tree, Random Forest, and Naïve Bayes) in terms of their accuracy, F1 Score, and Precision was evaluated.

Related work

The main part of our work is a trusted algorithm, particularly for DDOS attacks, which is considered best for years by well-recognized authors. There are a lot of machine learning algorithms for curing these DDOS Attacks Mehdi Barati preferred ArtificialNeural Network (ANN) and Genetic Algorithm (GA) for selecting features and attack detection individually in hybrid method and discovered that in terms of recall,accuracy, and precision their research approached the most accurate results as compared to previous studies. It was 2014 so after that, many new attack types has been discovered and so many new methods have been deployed for detection or prevention after that Alan Saied [2].

In 2016, an artificial neural network (ANN) algorithm was selected based on accurately distinguishing features (models) to detect DDoS attacks and separate DDoS attack traffic from traffic. Genuine [3].

Then in 2020 Meng Wang∗, Yiqin Lu, and Jiancheng Qin preferred the multilayer perceptron (MLP) to determine and explain the proposed problematic attack. In their solution, for extracting the best features in the training section they shared sequential feature selectionwith MLP, and a feedback mechanism was introduced to recreate the detector when perceiving significant Detection errors dynamically. The results presentedthat the proposed technique could correct the detector when it performed unwell and can profit detection routine [4].

Artificial intelligence plays a vital role in every field. There are various number ML algorithms available to detect the performance of models. The authors compare the performance of 5- widely used algorithms for text classification. It was observed that Logistic Regression works efficiently [5]. Several studies have been done in the field of DDOS Attacks and are considered important for Cybercrime etc. The authorsto prevent, Attacks and the techniques for such types ofattacks, performed a survey. The authors discuss interesting facts [6].

The development of webpages makes it easier for an attacker to attack through different sources such as Advertisement, Network Traffic, HTTP Request, Cookies, etc. and the researchers had discovered number a of tools to detect these attackers the authors discuss OWASP ZAP tool to detect attacks and level ofRisk concerning different parameters. A comparisonwas done between OWASP, ARACHNI, and WAVESEP tools, and was concluded that the OWASP tool performs better than the others [7].

Methods and Materials

The main objective of this research study is to proposea framework to detect DDOS attacks using Machine- learning algorithms. The OWASP ZAP and WEKA toolwas used. The research study was performed in thefollowing ways.

Step-1

This first and initial stage of the framework comprises two main levels namely traffic level and User level. Initially, a connection request will be sent to the server. After a successful establishment of connection, only after that, a user will be applicable to achieve various resources from the server. Many users will have to send the connection request to the server simultaneously and continuously. Incoming traffic from the user as well as traffic level will be monitored on the server side. Through monitored attributes which are historicalweblogs and real-time, weblogs of a server DDOS attacks will be detected. After successful detection, the impact on legitimate users can be minimized by filtering attacked traffic.

Step-2

Loading Dataset at WEKA tool and apply feature Selection and finally apply Algorithms to compare the performance of algorithms (Naïve Bayes, Decision Tree, Random Forest, SVM) in terms of Accuracy, Precision, and F1 score, Recall was evaluated and compared [8].

The experiment was done on Intel (R) Celeron(R) CPU 3867U @ 1.80GHz 1.80 GHz and 4.00 GB RAM.

Results and Discussion

This research study proposes a framework for the detection of DDO attacks over the network by using the OWSAP ZAP tool and evaluate the performance of 4-widely used Machine learning algorithms (Random Forest, Decision Tree, Naïve Bayes, and SVM) concerning Accuracy, Precision, and F1 score. 1031 samples were collected, and the results are discussed below in Steps.

Step-1: Detecting and Monitoring Attacks.

Table 1 describes the URLs that have been used for attacks to obtain the parameters, protocols, Risk, and Confidence level of an attack.

Table 2 describes the level of vulnerabilities detected by the OWASAP tool. There are 4- types of Alerts for Risk High, Low, Medium, and informational generated by the tool depending on the different parameters such as Cookie without secure Flag, Absence of Anti-CSRF.

Serial No	URLS
1	https://aws.amazon.com
2	https://github.com/
3	https://www.ebay.co m/
4	https://www.muet.edu.pk
5	http://www.fb.login.com

Table 1: General Description of Websites.

Serial No	High	Low	Medium	Informational	Scanning Time
1	20	100	100	20	40 minutes
2	10	50	150	10	30 minutes
3	30	130	150	30	20 minutes

Table 2: Level of vulnerabilities.

WebsiteName	DDOS Attacks Types			
	Cross-site	CSRF Token	Application Disclosure	SQL injection
Amazon	32322	21	283	2042
GitHub	4	65	908	1127
eBay	1	269	0	206
MUET	2	0	400	430
Facebook	492	799	87	148

Table 3: DDOS attack types for each website.

The above table 3 describes the DDOS attack detected by each website along with their instances. It can be observed that the highest type of attack was found to Cross Site Scripting and the Amazon websites attain this attack at a high level. It can be seen from the above table that eBay has the lowest attack with Application Disclosure. There were many types of attacks detected but those attacks were found common on every website.

The description in table 4 is discussed below.

Cross-site scripting

This type of attack is done on the client side of a web application. By writing JavaScript malicious script injected through a web browser by an attacker by writing JavaScript. When the attacker visits the webpage that was coded the script will be executed.

S. No	DDOS Attack
1	Cross-site Scripting
2	Cross-site request forgery (CSRF)
3	SQL injection
4	Application Error Disclosure

Table 4: Detection of DDOS attacks.

Cookie, session tokens, and other sensitive data normally stole by an attacker. Through this, the contents of the website can be modified. The Reflected XSS, DOM, and Stored XSS are considered types of Cross-site scripting.

Cross-site request forgery (CSRF)

This type allows the attacker to perform an action that the users do not want to perform. For example, to change the email address on their account, or to change passwords or transfer funds, etc. to generate these types,need to write an HTML script and make attacks through Http Links.

Token, Application Disclosure, CSRF Token, Cross- site, etc. concluded that most Medium Risks was detected.

SQL injection

This type allows malicious SQL statements and this statement controls the database of an application i.e one can go through authorization to add, modify, and records and may be contents of the webpage. Sometimes criminals may steal sensitive data including customers' personal information, property, records, etc. using SQL databases language such as MYSQL, Oracle, and SQL servers, etc. this type is considered the oldest and most dangerous attacking method.

Application error disclosure

In this type of attack, users' data cannot be protected. This is an easy way to hack users' information. Information includes server environment credentials, API, and many more. Banner grabbing; source code disclosure, file name, and path disclosure are the types of Application Error Disclosure.

Prevention techniques

It was observed in 2020 by the Kaspersky Lab survey that attacks increased by 80%. Attacks from DDoS can overwhelm data centers, driving up service provider costs. During a Dos attack, such as a flood attack, usersmay experience lengthy downtime and connectivity issues. The following steps might be useful for avoiding an attack:

- Developing tactics to deal with those services.
- Preserving the network's resources.
- Filtering firewalls & routers at the networkscan block and detect the link.
- Routing all traffic to an invalid IP address,black holing the DDoS-attacked site.

Step-2: Evaluation and performance of algorithms

The dataset contains URLs, Confidence level, Risk Level, protocol, and parameters and after uploading, the dataset was split into 80% for training and 20% for testing.

Accuracy

The ratio of appropriately forecasted observations to the total observations.

A = TP + TN/TP + FN + FP + TN-- ----------(a)

Precision

The proportion of accurately forecasted positive observations to the total number of positively forecasted observations.

P = TP/TP+ FP--------(b)

Recall

The ratio of correctly expected positive observations to all observations in a definite class is known as recall.

R = TP/TP+ FN ----------(c)

True positives (TP)

These are the data points whose real consequences were positive and the algorithm appropriately identified them as positive.

False positives (FP)

These are the data points whose real consequenceswere negative, but the algorithm wrongly identified them as positive.

Figure 1 shows the performance of Naïve Bayesalgorithms. It can be said that the algorithm achieved 85% of Recall as well as Accuracy, while 80% ofPrecision and 89% F1 Score.

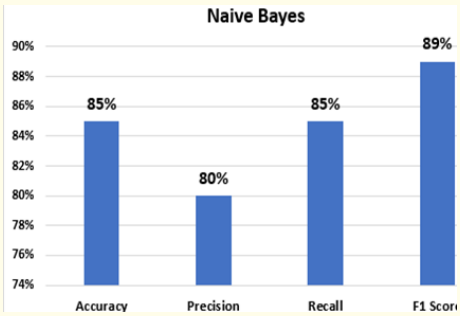

Figure 1: Performance of Naïve Bayes.

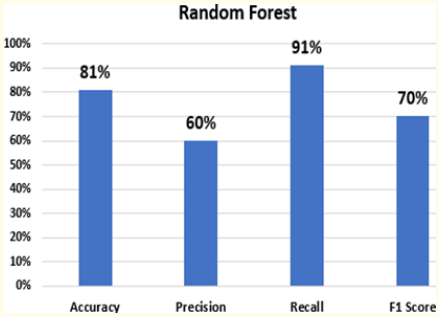

Figure 2: Performance of Random Forest.

Figure 2 shows the performance of the Random Forest algorithm. The algorithm obtained 81% of Accuracy, 60% of Precision, 70% of F1 score, and 91% of Recall.

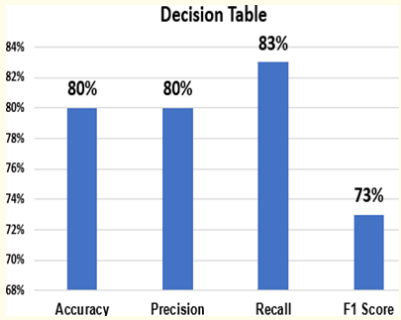

Figure 3: Performance of Decision Table.

Figure 3 depicts the performance of the Decision Table algorithm and can be concluded that the algorithm achieved 80% of accuracy, 73% of F1 Score, 80% of precision and 83% of Recall.

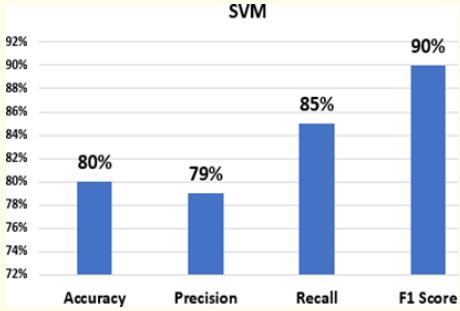

Figure 4: Performance of SVM.

Figure 4 illustrates the performance of the SVMalgorithm. The algorithm attained 80% of Accuracy, 79% of Precision, 90% of F1 score, and 85% of Recall.

Figure 5 discuss the performance of the algorithm and based on the nature of the dataset it can be observed that theNaïve Bayes algorithm achieved the best performance while Random Forest attained the highest Recall.

Conclusion

This research study presents a framework for the detection, Monitoring and providing Prevention techniques of DDOS Attacks utilizing ML algorithms. The performance of the four most extensively used algorithms was examined in terms of Recall, Precision, F1 score, and Accuracy. OWASP Zap Weka Tool was used for the analysis. The 5-famous websites namely, Amazon, GitHub, eBay, MUET, and Facebook were preferred for the attack. 1031 samples were collected.It was observed that most websites have a Medium Type of Risk and was observed during the study that the Amazon website captures a high type of Risk but a medium level of Confidence. In addition, studies relieved that Naïve Bayes Algorithms

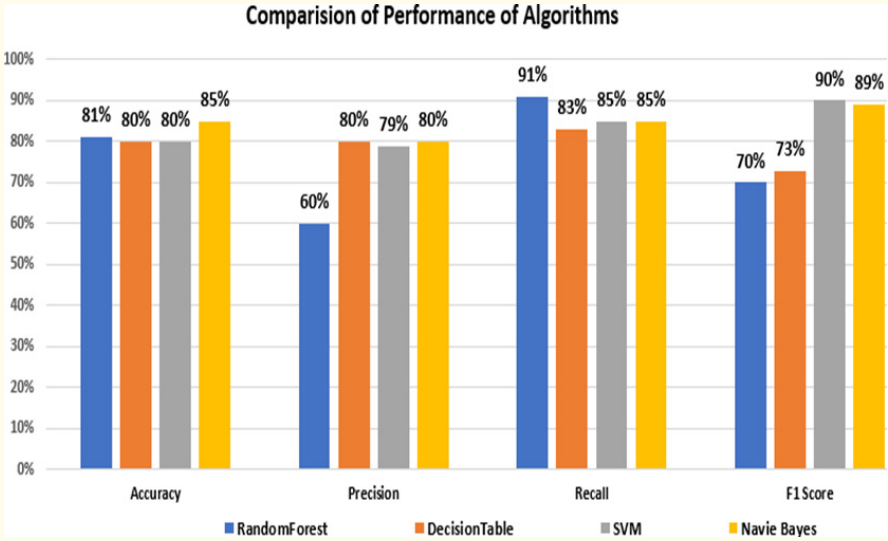

Figure 5: Comparison of all algorithms.

and RandomForest works efficiently for detecting attacks over the URLs with ratios of Accuracy, Precision, F1 score, and Recall. XSS, SQL injection, CSRF, and CSP Wildcard directive were observed as attacks.

Bibliography

1. Iman A and Mamdouh A. "Efficient Denial of Service Attacks Detection in Wireless Sensor Networks". *Journal of Information Science and Engineering* (2018): 977-1000.

2. Barati M., *et al*. "Distributed Denial of Service Detection Using Hybrid Machine Learning Technique". *International Symposium on Biometrics and Security Technologies (ISBAST)* (2014).

3. Saied A., *et al*. "Detection of known and unknown DDoS attacks using Artificial Neural Networks". *Neurocomputing* (2016): 385-393.

4. Wang M., *et al*. "A dynamic MLP-based DDoS attack detection method using feature selection and feedback". *Computers and Security* (2020).

5. Pranckevičius T and Marcinkevičius V. "Comparison of Naïve Bayes, Random Forest, Decision Tree, Support Vector Machines, and Logistic Regression Classifiers for Text Reviews Classification". *Baltic Journal of Modern Computing* 5.2 (2017): 221-232.

6. Mahjabin T., *et al*. "A survey of distributed denial-of-service attack, prevention, and mitigation technique". *International Journal of Distributed Sensor Networks* 13.12 (2017).

7. Mburano B and Si1 W. "Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark" (2019).

8. Hall M., *et al*. "The WEKA Data Mining Software: An Update". *ACM SIGKDD Explorations Newsletter* (2014).

9. Ji S Y., *et al*. "A multi-level intrusion detection method for abnormal network behaviors". *Journal of Network and Computer Applications* (2016): 9-17.

10. Yusof A R., *et al*. "Adaptive Feature Selection for Denial of Services (DoS) Attack". IEEE Conference on Application, Information and Network Security (AINS) (2017).

11. Guri M., *et al*. "DDoS: Attacks, Analysis and Mitigation". IEEE European Symposium on Security and Privacy (2017).

12. Chadd A. "DDoS attacks: past, present and future". Network Security, 2018 Elsevier, Network Security (2018): 13-15.

13. Filho LdsF., *et al*. "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning" (2019).

14. Manavi TM. "Defense mechanisms against Distributed Denial of Service attacks: A survey". *Computers and Electrical Engineering* (2018): 26-38.