Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023)
IEEE Xplore Part Number: CFP23P17-ART; ISBN: 978-1-6654-7467-2

DDOS Attack Detection with Machine Learning: A Systematic Mapping of Literature

2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) | 978-1-6654-7467-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSSIT55814.2023.10060897

Shreya Singh
Department of Information Technology
IGDTUW
Delhi, India
shreya020mtit21@igdtuw.ac.in

Megha Gupta
Department of Computer Science
MSCW, University of Delhi
Delhi, India
meghabis@gmail.com

Deepak Kumar Sharma
Department of Information Technology
IGDTUW
Delhi, India
deepaksharma@igdtuw.ac.in

***Abstract*— This is an era where at every stretch a person is becoming susceptible to a cyber attack. To avoid these cyber attacks or prevent people from becoming a victim of malicious attacks, various technical measures have been taken. Various research has been conducted on the detection and prevention techniques. Machine Learning plays a major role in detecting cyber-attacks. This paper discusses about Distributed Denial of Service Attack (DDOS). These are one of the harmonious malwares that intend to increase the false network traffic resulting in engulfing the targeted website. As the technology advancing these types of attacks have been forming its types in the form of size, traffic and modes. On analyzing the research paper different algorithms like Random Forest, Convolution Neural Networks etc. have been implemented on different datasets. Some research papers divided the dataset into two parts and implemented the machine learning algorithms to get good precision and accuracy. Some researchers implemented two approaches: one the mathematical model and other is the machine learning model. Through these models a throughput analysis was done to have a better accuracy, resolution time and precision of the proposed model. This paper discusses about all such research work done in this field and provides a detailed analysis of the DDOS attacks detection algorithms.**

Keywords*— *Cybersecurity, DDOS, IOT, intrusion detection mechanisms, machine learning, SDN.

I Introduction

The major peril faced by this world is cyber threats. The users of the Internet are growing day by day. Internet has been used as a medium of gaining information but on the other hand, internet is also acquiring the data. Internet has its own uses but it has too many loopholes as well. The data which is saved in the electronic devices has been passed through the network, hence acting as a door for cyber-attacks. Nowadays, security is the greatest concern for all internet users. The apps or the sites used or the cookies accepted will store the user data for delivering a better customization. Still there are sites, which are made for the sole purpose of performing malicious activities. For this reason, cybersecurity came into existence. A triad was designed to prevent cyber-attacks. CIA triad stands for Confidentiality, Integrity and Availability [1]. Confidentiality means regulations framed to restrict the access of data to legitimate individuals only. Next comes the integrity, it keeps a check that the data has not been modified. Then comes availability, it ensures that data is readily available to the users and prevents any bottleneck. This triad comes into role when the data is being sent. In the process of transmission, the attacker's main aim is to capture the data using different cryptographic algorithms. Using these cryptographic algorithms, the defenders use encryption techniques to protect the password while the attackers try to decrypt it using various decryption algorithms. As the attacks are increasing day by day the cyber criminals have started giving these attacks as services. These attacks are caused using transmission through the network. As the excessive use of the internet has caused the generation of more network logs which is difficult to analyze manually. Most of the systems like Intrusion Detection and Intrusion Protection have different patterns. To solve all these problems and prevent sophisticated attacks here comes the role of machine learning. Anomaly detection is used to detect these attacks. Anomaly detection is used in identification of the data points that don't fit the normal patterns. It is used to solve many problems like fraud detection and is very effective when large datasets are involved. Machine learning is being incorporated with cybersecurity to respond against all the cyber attacks. Currently, the main focus of the entire nation is on finding an automated security model which detects all threats which were detected before and can be generated in future. As technology is advancing day by day, machine learning plays a major role in cybersecurity. One such major role is preparing a machine learning model to detect a cyber-attack. Machine learning is a process that learns on a well-defined task T over experience E as measured by performance metric P. Machine learning algorithms allow the system to work autonomously. Based on the input, output and the type of problems they solve, the learning is of three types [2]:

- Supervised Learning: The system or model is trained and is well labeled. On the basis of that, data machine predicts the output.
- Unsupervised Learning: In this a raw dataset without any labels is used to train the model.
- Semi-supervised Learning: It lies in between the supervised and unsupervised learning.
- Reinforcement Learning: It's a feedback-based method in which an agent gains experience by performing actions and observing the output of the actions.

These supervised and unsupervised algorithms have sub algorithms which plays an important part in proposing the model and calculating its accuracy.

II Background

A. *Basics of Cybersecurity*

Threat is the violation of security. The violation of rules occurs because of the actions and we should be prepared with preventive measures to avoid any damage. These are called attacks and are headed by a malicious attacker or an iniquitous person. Threats can be classified as [3]:

- Snooping - It is a kind of violation of disclosure agreement which explains that an individual who can be a malicious attacker is listening or reading our private texts and is trying to gain access through unauthorized ways.
- Masquerading or spoofing- It is a process in which a malicious attacker tries to gain unauthorized access by making the user feels that it is a trusted entity or person.
- Denial of Service - It is the process in which the iniquitous person prevents the server from delivering the respective service. This attack can occur at the source end, or the destination end or the intermediary path. It is equivalent to a longer delay than expected. This threat is countered by availability.

B. *Encryption and Decryption*

Whenever we talk about security, encryption and decryption plays a major role. To have control of the other system, the attacker tries to decrypt the key which is encrypted by a password. The confidentiality can be achieved using encryption and decryption. The encryption process involves plain text (P) which is the original message and the ciphertext(C) which is the scrambled message. The ideology of message is implemented by the sender in order to protect the data from any malicious activity. Cryptosystems can be divided into two types [4]:

- Symmetric Cryptosystems: In this the sender and receiver both uses a common key for encryption and decryption.
- Asymmetric Cryptosystems: In these two keys has been used, private and public key for encryption and decryption.

C. *Basics of DDOS Attack*

In [5], DDOS is a malicious attack used by the hackers to make network devices or host servers or machines unavailable to the users. Implementation of this attack involves multiple online connected compromised devices.

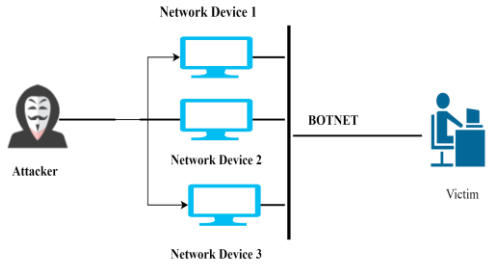

Fig1 :DDOS Attack

Fig 1 illustrates DDOS attack. The attack illustrated by the figure is a type of flood attack. The mandatory condition for this attack to be successful is that the attacker or iniquitous person should have a sufficient amount of bandwidth.

D. *BOTNETS*

In [6], BOTNET is a group of devices that are connected to the internet and gets compromised by the attacker to perform a malicious activity. These devices are remotely controlled by the hacker. The devices controlled by the attacker are known as bots and the group of each device is referred to as BOTNET. The range of the devices can be from hundred to millions which helps the hacker to perform wide range of criminal actions. Once large numbers of devices are compromised the attacker can use different approaches. The first approach is client server BOTNET which involves the establishment of a command-and-control server. Then automated commands are sent from the control's server to the compromised devices or BOTNET through various communication protocols. The other approach used is P2P Botnet which involves peer to peer connection of compromised devices. In this approach, no central server is present, and the bots or infected devices acts as a sender and receiver simultaneously. In [7] there are signs that explain your device has been compromised and become a part of the BOTNET: i) the processors, hard drive are running excessively without any reason, ii) slow internet speed, iii) automatic shutdown of your device, iv) crashing of applications, v) BOTNETS use a lot of memory, so check the percentage of your RAM, vi) Span emails – people start complaining that you sent them a malicious email.

E. *Working of DDOS attack*

DDOS attack is brought into function by compromising the sources of the network which are connected through the internet or forming a BOTNET as shown in Fig 2. Now as the BOTNET setup is complete, the bots check for other systems which are vulnerable and injects a virus or malware into them. When the targeted server's network is detected and there are enough infected devices, a command comes from the server which instructs the bots to start sending large number of requests, resulting in flooding of the network. When too many systems are attacking the targeted network, it results in slowdowns or service disordering [8]. As the attack is functioned with the help of internet connected devices because of that there are lot of complications faced in differentiating between normal and malicious traffic.

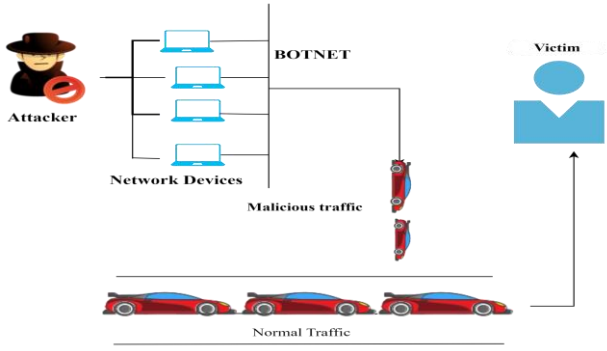

Fig 2: Operation of DDOS Attack

F) Types of DDOS attack

In [9], DDOS attacks are classified as: Volumetric Attacks, TCP State Attacks and Application Layer Attacks. Volumetric Attacks: - It creates traffic by sending huge data causing the destruction of bandwidth. These attacks are also known as connectionless attacks. TCP State Attacks: - or protocol attacks. This attack causes service disordering by slowing down the network resources and the server resources as shown in Fig 3. This network resource includes firewalls and load balancers. These attacks are also known as exhaustion attacks or network layer attacks.

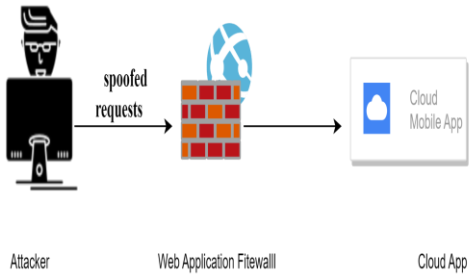

Fig 3**:** Application Layer Attack

Application Layer Attacks: - It is one of the most dangerous attacks. In the above figure 3, the iniquitous person sends spoofed HTTP requests to application. The attacker aims to send numerous requests to the user's server which loads the system and disrupts the application services. But if we impose a web application firewall before the application it will filter the malicious traffic sent by the attacker to a greater extent based on the previous patterns of the traffic and block them from getting in contact with the application's confidential data.

G) Recognition of DDOS Attacks

In [10], the model uses joint entropy feature and takes advantage of Tasllis entropy and Extreme Learning Machine. The joint entropy feature is extracted which reflects the DDOS attack charactersticks. The dataset is generated in real environment. The feature extraction of the dataset by the extreme learning machine resulting in distinguishing the normal DDOS attack flow and false positive rate of DDOS attack detection. In [11], the model uses two algorithms: Naïve Bayes and Random Forest. The Naïve Bayes algorithm calculates the conditional probability with the help of Gaussian probability density function. The class with the maximum probability is chosen. The Random Forest works used generates multiple decision trees. The dataset used consists of malware dataset and legitimate dataset. The prediction of the DDOS attack in the network is done using a malware variable which states that 0 is a legitimate access and 1 is malicious access or DDOS attack access.

H) Prevention of DDOS attacks

In [12], the model comprises of four phases: Network Model, Good and Attack Traffic Generations, Push Back Mechanism and last is client puzzles. This model is a hybrid model for prevention of DDOS attack which identifies the host and pushes back the host address to the upstream router. The upstream router on receiving the request with suspected address and gave them a puzzle. If the suspected host is not able to solve the puzzle, the upstream router confirms that it is an attacker, and the edge traffic blocks all the traffic from the attacker. In [13], the use of honeypots is described. It has been observed that the honeypots act like a legitimate system and leaves an impression on the attacker of hacking the legitimate system. The use of honeypots has resulted in protection of various devices from DDOS attack.

III RELATED WORKS

This section is going to discuss various authors' work describing machine learning algorithms in three environments: Software defined Networking (SDN), Internet of Things (IOT) and Cloud Computing.

A MACHINE LEARNING ALGORITHMS TO DETECT DDOS ATTACK IN SDN

A comprehensive study on the ML techniques to detect DDOS attacks has been provided by Sahoo et al. [14]. This paper figured out numerous approaches to detect DDOS attacks in a SDN network. In [15], support vector and decision tree are used for detection of DDOS attacks in a SDN environment. Here, a tool MININET is used to establish a topology network. Using MININET, around 100 hosts, 9 switches and 3 controllers were incorporated. Support vector and decision tree are used to distinguish between the normal traffic and the one sent by the attacker. On observing the results, Support Vector Machine (SVN) shows better results than Decision Tree in the SDN environment. The accuracy achieved by SVM is 85% and by Decision Tree is 78% in SDN environment. In [16], machine learning algorithms are used in detection of the two datasets. The algorithms are tested on already recorded and self-recorded datasets. In this a model was proposed which uses a simple supervised learning technique to detect DDOS flooding attacks. Four supervised algorithms: K- Nearest Neighbours, Decision Tree, Feed forward Neural Network and Bagging Tree were used. To have a valid accuracy all the algorithms were tested for CPU consumption and response time. On observing the results, the accuracy came out to be 99.64% which was achieved by bagging tree. In [17], a model was proposed which aims at rapid detection of DDOS attacks. The model was that the requests coming from the real time dataset were compared with the trained classifier. If the values match with the trained classifier, then the incoming request will be mentioned as normal traffic and if it doesn't match then it will be considered as an attack or malicious traffic. The three algorithms which were employed in the proposed model are Decision Tree, Naive Bayes and Logistic Regression. In [18], a model was implemented using K-means and Random Forest for detection of DDOS attacks in software defined networking environment. The method employed in this paper consists of two steps. The first step involves a combination of clustering and classification methods and the second step is detection method using Mininet Emulator. After performing these algorithms on the dataset, ensemble K++ and random forest which was the first stage of the first step of the proposed model proved out to be more efficient than the ensemble clustering and classification method in the second

stage of the first step. In [19], this research paper concludes that deep neural networks are an efficient algorithm to detect DDOS attacks. While observing the results this algorithm achieved an accuracy of 92.30%. The second algorithm used in this paper is support vector machine which achieved an accuracy of 74.30%. In [20], the paper discusses that deep learning is playing a major part in detection of DDOS attacks. This paper aims to avoid malicious traffic using binary classification problems. This experiment was performed on an NSL-KDD dataset and concludes that machine learning algorithms should keep advancing to propose new efficient models to deal with DDOS attacks. In [21], the model was proposed using two deep learning methods. The model was divided into two parts: one part is the autoencoder part which implements the feature extraction algorithm to find the most accurate and relevant features. The second part is a multi-layer perceptron network that classifies the features identified by autoencoder into different types of DDOS attack. In [22], this paper aims on the types of volumetric attacks i.e. the ICMP, TCP and UDP attacks. These attacks target the controller as it is the only thing to be attacked and the only vulnerable source in the whole network. The result showed that RNN LSTM will be the best choice for the DDOS attack and promotes an accuracy of 89.63%. In [23], support vector machine learning algorithm is used to know the nature of the traffic whether malicious or normal and proceed with the detection of DDOS attack. The accuracy for the model implemented was 95.24% with an average false rate of 1.26%.

B MACHINE LEARNING ALGORITHMS TO DETECT DDOS ATTACK IN IOT ENVIRONMENT

In [24], Naive Bayes, Decision Tree, Random Forest and ZeroR classifiers were compared. In this Principal Component Analysis was employed to use feature extraction. Then the performance of these classifiers was tested on the filtered data through PCA technique. This model also employed a WEKA tool to use machine learning algorithms. In [25], this paper detects an abnormal activity in IOT devices. The model is divided into four phases: dataset loading, dataset pre-processing, remembering the patterns of the normal and abnormal dataset and the last phase is the testing phase. It was found that the random forest and decision tree achieved the highest accuracy in identifying DDOS attacks. In [26], the paper dictates that machine learning applied at packet level can distinguish normal and malicious traffic. All the five algorithms K-nearest neighbor, SVM, Decision Tree, Random Forest, Neural network were used to fulfill the purpose. Ambrish et.al. [27], the dataset consists of 88 features out of which 15 features were extracted. The four algorithms used in the proposed model are ANN, K-nearest neighbours, Random Forest, Decision Tree. In [28], the components used in this model are data pre-processing, supervised learning, semi-supervised learning, unsupervised learning and prediction. All the five techniques were tested for accuracy and prompted in detecting DDOS attacks. In [29], this paper is a review of the type of DDOS attacks that can be implemented in IOT networks. It also discusses the various solutions, problems, limitations in detection of DDOS attack. In [30], a service-oriented architecture has been used that determines to make the model completely free from DDOS attack. To protect every layer of DDOS attack, the concept of cross layer is applied. On the application of Learning Automata implemented in this model, there were less malicious requests observed than in its absence. In [31], the aim of this paper is to detect any malicious attack observed using the Matrix profile. The matrix paper calculated using sliding window or receding horizon algorithm. The main objective of using matrix profile is to see discrepancies in time series datasets. In [32], 10 relevant features were extracted from the dataset. The machine learning algorithms which were used to detect the traffic were Random Forest, Logistic Regression, Decision Tree and Naive Bayes. In this paper, Elimination Et Choix Traduisant la REalite method (ELECTRE III) is used to record the ranking of the selected algorithms. On implementing the model, Random Forest achieved the highest accuracy. In [33], it has been discussed that IOT devices process a large amount of data and are the most vulnerable to attacks. This paper also talks about the DDOS attack which was done on Austrian and German power grids. The service of these power grids was disrupted which resulted in optimization loading of malicious traffic of the central command centre.

C MACHINE LEARNING ALGORITHMS TO DETECT DDOS ATTACK IN CLOUD COMPUTING ENVIRONMENT

In [34], three machine learning classifiers: Naive Bayesian, C4.5 and K- means were used. Out of the three classifiers, C4.5 was considered the best algorithm as it has the highest accuracy out of the three classifiers. In [35], the paper concludes that Dempster Shafer Theory (DST) in 3 valued logics when applied on the proposed logic resulted in a smaller number of alerts. It also reduced false negatives and increased the detection rate of DDOS attacks. In [36], two datasets NSL-KDD, KDD Cup 99 were used. The proposed method consists of radial base function (RBF) with particle swarm (PSO). This combination was used to identify the flood type DDOS attack. On implementing the model, the performance metrics of above 85% was achieved. In [37], the dataset used was an input to the Intrusion Detection System SNORT. The model was implemented in cloud stack environment. The accuracy of the five algorithms: Decision Tree, Random Forest, Naive Bayes, SVM and C4.5 were used to test the model. In [38], this paper is a comprehensive review which discusses the security vulnerabilities, attack scenarios and ML techniques based on Anomaly detection System. In [39], the aim of this paper is to detect HTTP type DDOS attack. HTTP type DDOS attacks are type of attacks that seem almost similar to normal attacks. In [40], the model comprises of two parts: Learning Vector Quantization (LVQ) and other is Principal Component Analysis. On observing the results, it came out that the decision tree is the best algorithm from the other two to detect DDOS attack in cloud computing environment. In [41], the approach uses a combination of Cuckoo Search and Artificial Neural Network Approach. It consists of a detection module which is connected to the router. With the help of router, the user is able to access the network services from the cloud server. In [42], WEKA tool is used to test and train the datasets. Results were that K -

nearest neighbour proved out to be the best for large datasets and Support Vector achieved proved out to be the best for small datasets. In [43], the study consists of the solutions which were used to detect DDOS attack. The model proposed uses Fuzzy Q Algorithm and Chebyshev's inequality principle to deal with DDOS attacks. The result depends on the state of the cloud environment i.e., good, bad and excellent.

The summarization of the machine learning models used for DDOS attack detection is mentioned in Table 1.

Table1: Description of the various Approaches

Algorithm, Dataset used And Detection Accuracy	**Merits and Demerits**	**Limitations**
Algorithm-Decision Tree[44] Dataset used – DDOS attack SDN Dataset Accuracy -100%	Merit- The dataset used is recorded in real time. Demerit – Implementation of the model will be difficult.	Difficult to have a general analysis of the model.
Algorithm-Random Forest [45] Dataset used– NSL-KDD dataset Accuracy-RF-99.97%	Merit-The combination of machine learning algorithms used protects the SDN controller. Demerit- Use of too many features may affect the efficiency.	The model can fail in multi-controller environment.
Algorithm-AdaBoost and XGBoost [46] Dataset used – CICDDoS2019 Accuracy – 100%	Merit –All the models presented in this paper prevents the risk of overfitting. Demerit-The dataset used has features which are dependent on each other which resulted in less accuracy of some algorithms.	No limitations
Deep Neural Network and LSTM [47] Dataset used - CICIDS2017 dataset Accuracy – DNN-98.72% LSTM-96.15%	Merit – This review paper gives a detailed overview of all the approaches. Demerit– Includes models which has very low accuracy which is of no use.	No limitations
Decision Table [48] Dataset used – UNSW-NB 15 Accuracy – 88.43%	Merit-Due to the use of information gain, computational time was less. Demerit-Model was implemented on one dataset only.	The efficiency of the dataset is limited to one dataset only.
Random Forest [49] Dataset used - NSL-KDD Accuracy – 99.76%	Merit – Has less computational time and good accuracy. Demerit- Model can be easily hacked when came in contact with a IP datagram.	The model is limited to one dataset and its accuracy can change with a different dataset.
Perplex Bayes Classification with Feature Selection [50] Dataset used – NSL-KDD Accuracy – 99%	Merit – Less implementation cost because of use of feature selection. Demerit –The model showed some misinterpretations while determining the data for regular as well as malicious attacks.	This model is not scalable. It can't be applied on different datasets and implemented in different environments.
Random Forest [51] Dataset used-CICDDoS2019 Accuracy-99.99740%	Merit- It can be easily handled, cost effective. Demerit - Not dynamic.	Operates on small datasets only.
Hidden Markov Model[52] using Random Forest Dataset used-KDD-Cup99 Accuracy – 97.34%	Merit – It provides the degree of attacks and reduces any type of noise. Demerit – It is a complex model and can't be implemented in every environment.	The model only works for low rate DDOS attacks.
Conventional Neural Networks [53] Dataset used – ISCXIDS2012 Accuracy – 99.35%	Merit - It is scalable and dynamic. Demerit - The use of autoencoders needs to be more explained and practically justified.	Insufficient amount of training data which can result in confusion of normal and DDOS traffic.
Logistic Regression, SVM, KNN, Decision Tree [54] Dataset used – NSL-KDD Accuracy – 90.4%	Merit - It plans to involve features which prevent the device from becoming a BOTNET. Demerit – Target chosen could have been more complex	This model is limited to one dataset and is not scalable.

	to prove the reliability of the model.	
Support Vector Machine[55] Dataset used – Dataset of Canadian Institute of Cybersecurity Accuracy – 97.1%	Merit – Clear justification of the attacks. Demerit - The reliability of the model is not justified.	It is not scalable and vulnerable to attacks.

IV OPEN ISSUES AND CHALLENGES

The open issues faced are that most of the proposed models were tested on a single dataset. If the model is tested for different datasets, it is a possibility that the accuracy of the algorithm will change for different datasets. So, it will be a major challenge to maintain the same accuracy for all the datasets despite what features they incorporate. Also, it was a tedious task for selecting and extracting optimum attributes for the ML models. The major issue while analysing the papers faced was to distinguish between the malicious and normal traffic as the traffic is made by a collection of legitimate network devices known as BOTNET.The attacker also sends spoofed IP requests which lead to the crashing of the system and this occurs before or during some important meeting which results in financial losses for many companies and even closing down of the companies at their initial stage.SDN has done lot of advancement in networking but the SDN controllers used is the central part of the network and is very vulnerable to DDOS attack.

DDOS Attack is the biggest issue and open challenge for all the business officials, internet service providers, or any fortune company.

V CONCLUSION AND FUTURE WORK

This paper involves the ML techniques to detect DDOS attacks. The methods were tested for three different environments to know which algorithm is most efficient and have high accuracy and it was observed in many papers that random forest acquires the highest accuracy in detecting DDOS attack. This paper illustrates the intention of attackers to disrupt the services of victims. This paper also defines the algorithms and the procedures that are being used to cure all types of DDOS attacks. At last, the paper will act as a base for the beginners in the subject of cybersecurity or new researchers who are looking for ideas to propose a new, innovative, effective and accurate model to detect DDOS attacks. In this paper, the models shared belong to SDN, IOT and Cloud Computing environments but in future an effort will be made to increase the scope of this model by including detection of DDOS attacks in other environments as well. More techniques will be added in the future to increase the scope of this paper which will also include the detection of flood type DDOS attack.

REFERENCES

[1] Mrs Ashwini Sheth, Sachin Shankar Bhosale, Mr Farish Kurupkar, “Research Paper on Cyber Security”, 2021.
[2] Ozer Celik, “A Research on Machine Learning Methods and its Applications,” Journal of Educational Technology and Online Learning, 2018.
[3]https://www.informit.com/articles/article.aspx?p=363728&seqNum=2, visited on 17/12/22.
[4]https://www.tutorialspoint.com/what-is-the-difference-between-symmetric-key-cryptographic-and-asymmetric-key-cryptography, visited on 17/12/22.
[5]https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/, visited on 17/12/22.
[6] https://www.techtarget.com/searchsecurity/definition/botnet, visited on 17/12/22.
[7] https://www.malwarebytes.com/botnet, visited on 17/12/22.
[8]https://sectigo.com/resource-library/how-does-a-ddos-attack-work, visited on 17/12/22.
[9]https://www.onelogin.com/learn/ddos-attack, visited on 17/12/22.
[10] Z. Li et al., "Research on DDoS Attack Detection Based on ELM in IoT Environment," 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), pp. 144-148, 2019.
[11] G. Ajeetha and G. Madhu Priya, "Machine Learning Based DDoS Attack Detection," 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), 2019, pp. 1-5.
[12] Saravanan kumarasamy, Dr.R.Asokan, “Distributed Denial Of Service (DDOS) Attacks Detection Mechanism,” International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.5, December 2011.
[13] N. Weiler, “Honeypots for Distributed Denial of Service,” in: Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, June 2002, pp. 109–114.
[14] K. S. Sahoo, A. Iqbal, P. Maiti and B. Sahoo, “A Machine Learning Approach for Predicting DDoS Traffic in Software Defined Networks,” International Conference on Information Technology (ICIT), 2018, pp. 199-203.
[15] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques," International Conference on Computer Communication and Informatics(ICCCI),2021,pp.15.
[16] Song Wang, Juan Fernando Balarezo, Karina Gomez, Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan, Muhammad Rizwan Asghar, Giovanni Russelo, “Detecting flooding DDOS attacks in software defined networks using supervised learning techniques ,” Engineering Science and Technology an International Journal,2022.
[17] Abbas Jasem Altamemi, Aladdin Abdulhassan, Nawfal Turki Obeis, “DDOS Attack Detection in software defined networking controller using machine learning techniques,”2022,pp2836-2844. [18] D. Firdaus, R. Munadi and Y. Purwanto, "DDoS Attack Detection in Software Defined Network using Ensemble K-means++ and Random Forest," 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2020, pp. 164-169,.
[19] K. B. V., N. D. G. and P. S. Hiremath, "Detection of DDoS Attacks in Software Defined Networks," 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), 2018, pp. 265-270.
[20] Mahmoud Said Elsayed, Nhien An Le Khac, Soumyabrata Dev, Anca Delia Jurcut, “Machine Learning Techniques for detecting attacks in SDN,”2019 .
[21] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu and S. Camtepe, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," in IEEE Access, vol. 9, 2021,pp. 146810-146821.
[22] Gadze, J.D.; Bamfo-Asante, A.A.; Agyemang, J.O.; NunooMensah, H.; Opare, K.A.-B, “An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers Technologies ,”2021, 9, 14.
[23] Jin Ye, Xiangyang Cheng, Jian Zhu, Luting Feng, Ling Song, “A DDOS Attack Detection Method Based on SVM in Software Defined Network.”2018.
[24] Amardeep Chopra, Sunny Behal, Vishal Sharma, “Evaluating Machine Learning Algorithms to detect and classify DDOS attacks in IOT,” International Conference on Computing Sustainable Global Development, 2021.
[25] M. H. Aysa, A. A. Ibrahim and A. H. Mohammed, "IoT Ddos Attack Detection Using Machine Learning," 2020 4th International Symposium on

Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2020, pp. 1-7.
[26] Doshi, R., Apthorpe, N., & Feamster, N. (2018), "Machine Learning DDoS Detection for Consumer Internet of Things Devices," IEEE Security and Privacy Workshops (SPW), 2018.
[27] R. Amrish, K. BavaPriyan, V. Gopinath, A. Jawahar, C. Vinoth Kumar. "DDOS Detection Techniques Using Machine Learning Techniques," Journal of IoT in Social, Mobile, Analytics, and Cloud, Volume 4, Issue 1, March 2022.
[28] Phecha Machaka, Olasupo Ajayi, Hloniphani, Malueke, Ferdinand Kahenga, Antonie Bagula, Kyandoghere Kyamakya, "Modelling DDOS Attack in IOT Networks using Machine Learning," 2022.
[29] Al-Hadhrami, Y., & Hussain, F. K. (2021). "DDoS attacks in IoT networks: a comprehensive systematic literature review." World Wide Web, 24(3), pp 971–1001.
[30] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena and M. S. Obaidat, "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things," International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 114-122.
[31] Mohammed Ali Alzahrani, Ali M. Alzahrani, Muhammad Shoaib Siddiqui, "Detecting DDOS Attacks in IOT - Based Networks Using Matrix Profile, "Applied Sciences, 2022.
[32] Leonid Galchynsky, Mykola Graivoronskyi, and Oleh Dmytrenko, "Evaluation of Machine Learning Methods to Detect DoS / DDoS Attacks on IoT," XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS-2021), December 9, 2021.
[33] Kishore Angrishi, "Turning Internet of Things (IOT) into Internet of Vulnerabilities (IOV): IOT Botnsts,"2017.
[34] M. Zekri, S. E. Kafhali, N. Aboutabit and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 2017, pp. 1-7.
[35] Alina Madalina Lonea, Daniela Elena Popescu, "Detecting DDOS Attack in Cloud Computing Environment," 2013 International Journal of Computers, Communications and Control (IJCCC) 8(1):70-78.
[36] Kanimozhi S, Radhika D," Detection of DDOS Attack using Machine Learning Algorithms in Cloud Computing," Turkish Online Journal of Qualitative Inquiry (TOJQI) Volume 13, Issue 1, July 2022: 2079-2088.
[37] Abdul Raoof Wani, Q.P. Rana, Nitin Pandey, "Machine Learning Solution for Analysis and Detection of DDOS Attack in Cloud Computing Environment," Int' Journal of Engineering and Advanced Technology (IJEAT), Volume-9 Issue-3, February 2020. [38] Gavini Sreelatha, A.Vinaya Babu,Divya Midhun -chakkarvarthy, "A Survey on Cloud Attack Detection using Machine Learning Techniques," Int'l Journal of Computer Applications (0975 – 8887) Volume 175 – No. 34, December 2020.
[39] Mohammed Idhammad , Karim Afdel , Mustapa Belouch, "Detection System of HTTP DDOS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest," Security and Communication Networks, vol.2018,13 pages,2018.
[40] C. Bagyalakshmi, Dr.E.S. Samundeeswari, "DDOS Attack Classification on Cloud Environment Using Machine Learning Techniques with Different Feature Selection Methods," Volume 9, No.5, September - October 2020 International Journal of Advanced Trends in Computer Science and Engineering.
[41] Ahmed Saeed Alzahrani, "An Optimized Approach-Based Machine Learning to Mitigate DDoS Attack in Cloud Computing, "International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 6 (2020), pp. 1441-1447.
[42] Suzaifa, Abdul Khader, Sareen Fathima, "Efficient Identification of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 9, Issue 1, January 2022.
[43] Animesh Kumar, Sandip Dutta, Prashant Pranav, "Prevention of DDoS Attack in Cloud Computing using Fuzzy Q – Learning Algorithm," .
[44] Tonkal, Ö.; Polat, H.; Başaran, E.; Cömert, Z.; Kocaoğlu, R. "Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking." *Electronics* **2021**, *10*, 1227.
[45] Muhammad Waqas Nadeem, Hock Guan Goh, Vasaki Ponnusamy and Yichiet Aun, "DDOS Detection in SDN using Machine Learning Techniques" Computers, Materials & Continua, DOI:10.32604/cmc.2022.021669.
[46] Alireza Seifousadati, Saeid Ghasemshirazi, Mohammad Fathian, "A Machine Learning Approach for DDoS Detection on IoT Devices", October 2021, License CC BY-SA 4.0.
[47] Mittal M, Kumar K, Behal S., "Deep learning approaches for detecting DDoS attacks: a systematic review. Soft comput." 2022 Jan 27:1-37. Epub ahead of print. PMID: 35103047; PMCID: PMC8791701.
[48] Muhammad Aqil Haqeemi Azmi, Cik Feresa Mohd Foozy, Khairul Amin Mohamad Sukri, Nurul Azma Abdullah, Isrezda Rahmi A. Hamid, Hidra Amnur., " Feature Selection Approach to Detect DDOS Attack Using Machine Learning Algorithms" Vol 5, No 4 2021.
[49] Sagar Pande, Aditya Khamparia, Deepak Gupta, Dang.N.H. Thanh, "DDOS Detection Using Machine Learning Technique" October 2020, Recent Studies on Computational Intelligence pp.59-68.
[50] Narendra Mishra, R.K. Singh, S.K. Yadav, "Detection of DDoS Vulnerability in Cloud Computing Using the Perplexed Bayes Classifier" Computational Intelligence and Neuroscience, 2022.
[51] Ebtihal Sameer Alghonson, Onytra Abbass, "Detecting Distributed Denial of Service Attacks using Machine Learning Models," International Journal of Advanced Computer Science and Applications, Vol.12, No,12,2021.
[52]S.R.Mugunthan, "Soft Computing Based Autonomous Flow Rate DDOS Attack Detection and Security For Cloud Computing" Journal of Soft Computing Paradigm (JSCP) (2019), Vol.01/ No. 02 Pages: 80- 90.
[53] Ahmed Latif Yaser, Hamdy M. Mousa, Mahmnoud Hussein., "Improved DDOS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder,"2022.
[54] Neeraj Patil, "DDoS Attack Detection and Botnet Prevention using Machine Learning," International Research Journal of Engineering and Technology (IRJET), Vol 9, Issue 11, 2022.
[55] Md Abdur Rahman "Detection of Distributed Denial of Service Attacks based on Machine Learning Algorithms,"International Journal of Smart Home Vol.14, No.2, 2020.