RESEARCH ARTICLE

DOI: 10.34256/ijcci2214

International Journal of Computer Communication and Informatics

Towards applying FCM with DBSCAN for Detecting DDoS Attack in Cloud Infrastructure to Improve Data Transmission Rate

T. Devi [a,*], N. Deepa [a], R. Karthikeyan [a], J. Bharath Sundararaman [a]

[a] Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India.

* Corresponding Author: devi.janu@gmail.com

Received: 28-02-2022, Revised: 06-05-2022, Accepted: 10-05-2022, Published: 16-05-2022

Abstract: Cloud is a pay-to-use technology which can be used to offer IT resources instead of buying computer hardware. It is time saving and cheaper technology. This paper analyzes the DDoS attack on cloud infrastructure and can be detected by using FCM with DBSCAN hybrid algorithm that classifies the clusters of data packets and detects the outlier in that particular data packet. The experimental outcome shows that the enhanced hybrid approach has better results in detecting the DDoS attack. The DDoS attack targets the main host of the cloud infrastructure by sending unwanted packets. This attack is a major threat to the network security. The FCM with DBSCAN hybrid approach detects outliers and also assigns one specific data point in clusters to detect DDoS attack in cloud infrastructure. By using this hybrid approach the data can be grouped as clusters and the data beyond the noise level can also be detected. This algorithm helps in identifying the data that are vulnerable to DDoS attack. This detection helps in improving the data transmission rate.

Keywords: Pay-to-use Technology, Cloud Infrastructure, FCM with DBSCAN Hybrid Algorithm, Network Security, Unwanted Packets, Vulnerable.

1. Introduction

Cloud computing enables users to access resources, servers, databases, and storage space and data centers via the internet. Cloud services are developed and managed by CSP (Cloud Service Providers) and work under the "pay-per-use" model (subscription format available for the cloud formats). The IoT (Internet of Things) services are growing on a vast scale and storing those raw data locally is becoming impossible so the need for cloud computing technology is popping out.

Nowadays, people are more familiar with the cloud concept, some of the famous cloud-based applications used by most of the people are YouTube, Facebook, Dropbox, Google Drive.

The term cloud computing was first coined by John MacCharty in the year 1961. In his speech at MIT he stated that "Computing can be sold as Utility, as Electricity and water" and after a very long time the technology was first implemented in the year 1999 by Salesforce.com. A survey conducted during the year 2022 says that almost 94% of enterprises already use cloud services. Xbox live, Google Stadia's were major gaming projects launched on the cloud platform that enabled users to play games without having them on their personal computer. These projects work under "pay-per-use" or subscription based [1, 2]. This saves the cost for buying high end graphic cards or gaming consoles.

Cloud services are categorized under three common models:

(i) IaaS (Infrastructure-as-a-Service)

IaaS service providing companies have their own data centers and hardware and enable their customers access those resources in return via subscription programs. Simply, IaaS handles computing resources, storage facilities and virtual machines required for the organization, thus reducing the build cost and workspace for the company.

(ii) PaaS (Platform-as-a-Service)

PaaS takes care of the development side of the applications where the user needs to handle only the application and the data. Other activities like testing, development, runtime will be in the hands of the PaaS service providing company.

(iii) SaaS (Software-as-a-Service)

SaaS is a combination of PaaS and IaaS with enhanced features. SaaS covers all the service through cloud including applications and data which are excluded in PaaS service. There are 3 sorts of cloud models: public, private and hybrid. The public model offers cloud services to their customers on their premises of the company. AWS, Azure falls under public model and private model is the famous model among companies as CSP build infrastructures as per the needs of their clients and it is accessible only by one organization or the client. A third- party service provider distinguishes the use of the services from public access (prevents unauthorized access). Private cloud offers customization and control. Based on the purpose and requirements the hybrid cloud uses both public and private cloud. Benefits of cloud computing includes: i) Saves cost and workspace for the hardware/Server ii) Flexibility, as cloud services are scalable according to the needs of the client iii) CSP provides high security to the data by data encryption.

1.1 Problems in Cloud

Cloud service providers undergo a lot of risks and challenges. Denial of Service attacks are the most common and CSP are particularly vulnerable to this attack. EDoS (Economically Denial of Sustainability) attacks are kind of DoS attacks focused on the economic aspects [3]. Cloud services are attacked in the aspect of triggering auto-scaling technique (storages expand as per the incoming traffic), resulting in the cloud consumers ending up paying a vast amount of money occupied by the attacker [4]. Clients of CSP experience downtime of serve major cloud-based companies undergo DDoS attacks: LinkedIn underwent attack in 2016 and almost 170

million user profile details were stolen from their cloud, Dropbox user details were stolen from their database in 2012 [5].

1.2. DDoS Attack

DDos (Distributed Denial of Service) is a malicious attack targeting a particular server available on the internet. The attack is executed by sending a large volume of requests to the server, attempting to slow down or to restrict the legitimate users [6]. The attacker executes these by remotely controlling a vast number of computers/ servers (Basically, an attacker can get access to a user's computer by sending malicious viruses through mail or web) and using them as bots, altogether called the BOTNET (an army of infected computers). With such a huge amount of computational power the attacker can flood with requests and take down the server. Attackers not only use computers as BOTNET, with the advantage of growing IoT devices, the attackers can get access to those devices easily and can enlarge their army of bots. Gaining access to IoT devices across the globe can give more computational power and help the attacker to target large organizations. (Figure1.1 explains about victims and weapons of DDoS).

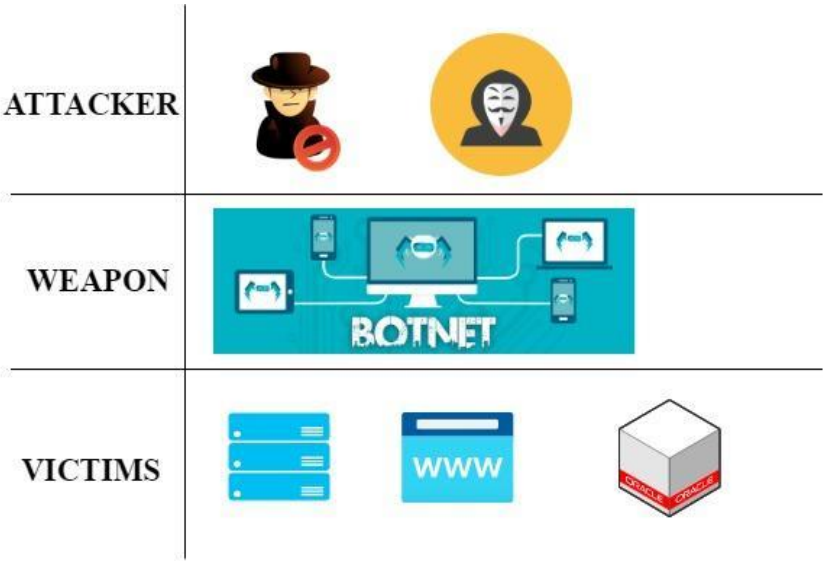

Figure1. DDoS Attack

Types of DDoS attacks - volumetric attack, Application layer attacks. DoS and DDoS are not the same, DoS (Denial of Service) encounters the target server from a single source. In October 2016, Dyn encountered a Mirai BOTNET attack which is more powerful than previous DDoS attacks and reports says that the company experienced a traffic of almost 1.2 Tbps done by thousands of IoT devices. Figure 1.2 shows the incoming traffic during DDoS attack.

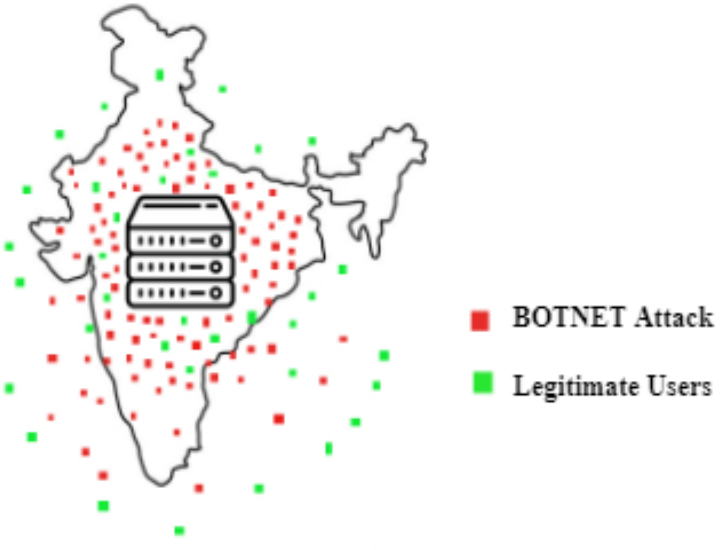

Figure 1.2. DDoS attacks on Servers

The objective the research work is

(i). To group the clusters of data using FCM (Fuzzy c-means clustering) algorithm.
(ii). To detect the outliers and noise data using DBSCAN (Density based Spatial Clustering of Applications with Noise) algorithm.
(iii). To detect the DDoS attack in cloud servers and improve the data transmission rate for the consumers.

The paper is organized as follows, Section 2 explains the existing works in the cloud environments, Section 3 elaborates the proposed work, Section 4 gives a detailed description on results obtained and Section 5 discusses the conclusion.

2. Literature Review

The existing works are discussed in the following sections, Auto-Scaling, a popular concept in cloud services provides dynamic resource utilization as cloud is based on a pay-per-use scheme. DDoS Attackers use these features to flood with traffic on the Virtual Machines. Attacks like these create greater impact on the financial aspects of the customers, as the attacker utilizes customer resources and these are called the Economic Denial of Sustainability attack (EDOS). EDOS attacks are mostly caused due to SYN flooding. CSP uses SDN technology to protect them from EDOS attacks. SDN classifies and separates incoming traffic and blocks them before the attack on the target VM (Virtual Machines). In order to overcome TCP SYN flooding attacks from spoofed IPs, the EDOS-TSM Model (EDOS-TCP SYN mitigation model) comes into effect [7].

Outsourcing of resources is one of the significant features of cloud computing which makes it to revolutionize the IT industry. At the same time, clouds suffer from various issues.

DoS attacks occur frequently and need to be detected to protect the data stored in the cloud. The system used for detection is based on three major algorithms as shown in Figure. The system works in two phases as (i) feature selection is performed using OCSA followed by (ii) passing it to classifiers like RNN (Figure 2.1 explains the three algorithms to detect DoS). Classification is done with the help of RNN followed by the process of removing the data that is compromised. The accuracy obtained from the proposed work is 94.12% and other parameters used are precision as well as recall [5].

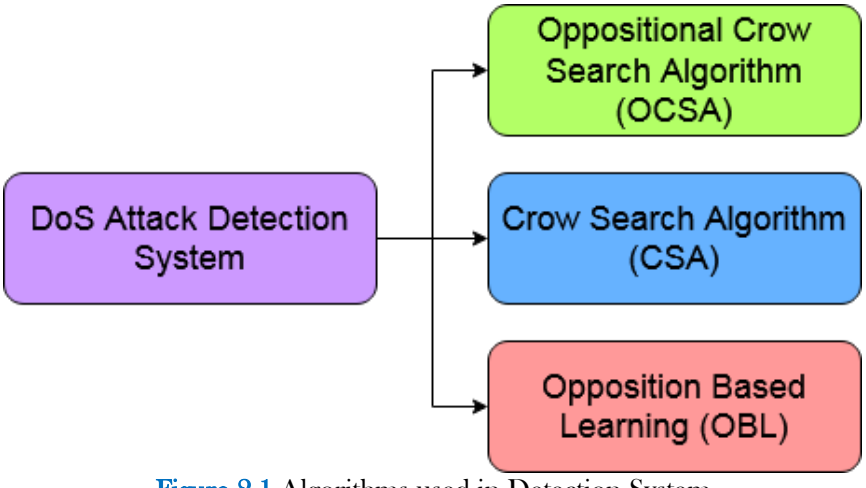

Figure 2.1 Algorithms used in Detection System

Cloud service provides enormous support to the client via the internet, but these servers are attacked in the intention of revenge or for competition among competitors. The most common attack on targeted victims is the ICMP (Internet Control Message Protocol) flood. Servers under ICMP flood experience heavy traffic, initiated by ping requests coming from a large volume of computers which are under the control of the attacker. A quick way to temporarily resolve this issue is by turning off the ICMP request on the server. But most companies use an auto- scaling technique, which enlarges their resources according to the traffic and the downside of this process is EDOS (Economic denial of sustainability), resulting in clients paying charges for the resources they haven't used [7]

Cloud computing provides the services managed by on-premises through cloud technology and they are very much vulnerable to malicious virus attacks DDoS attacks are some of the common attacks faced in the field of cloud technology [8]. DDoS attacks bring forth a huge amount of loss to the attacked company or the service. The taxonomy of the solutions to DDoS attacks are categorized under three branches i) Attack prevention ii) Attack detection iii) Attack Mitigation. So, it is important to prevent DDoS attacks beforehand, like implementing preventive measures when suspecting heavy traffic than usual [9]. When all the preventive mechanisms fail, the attack can be found under attack detection via traffic flow record analysis and can be resolved before it turns more vulnerable. When all these are penetrated by the attacker then the organization tries to allow access to their legitimate users by keeping the server active during the attack [10].

People of this era rely more on "Internet of Things" (IoT) devices for day-to-day activities and operations. DDoS attacks performed by an army of IoT devices with a BOTNET called the "Mirai". Mirai is basically a malware that hijacks the IoT devices (IP cameras, medical devices, agricultural devices), these devices can be used as BOTNET to overwhelm the target network and make it offline. Mirai takes over IoT devices, which still uses default usernames and passwords. Even Though IoT have small computational powers but these attacks would reach hundreds of tb/s. IoT devices are less secure and attackers gain access easily. These Mirai BOTNET problems can be given remedy by software-defined networking and fog computing. Large scale IoT attacks can be penetrated by SDN (Software Defined Networking) technique and follows a mechanism called "thin computing" [11]

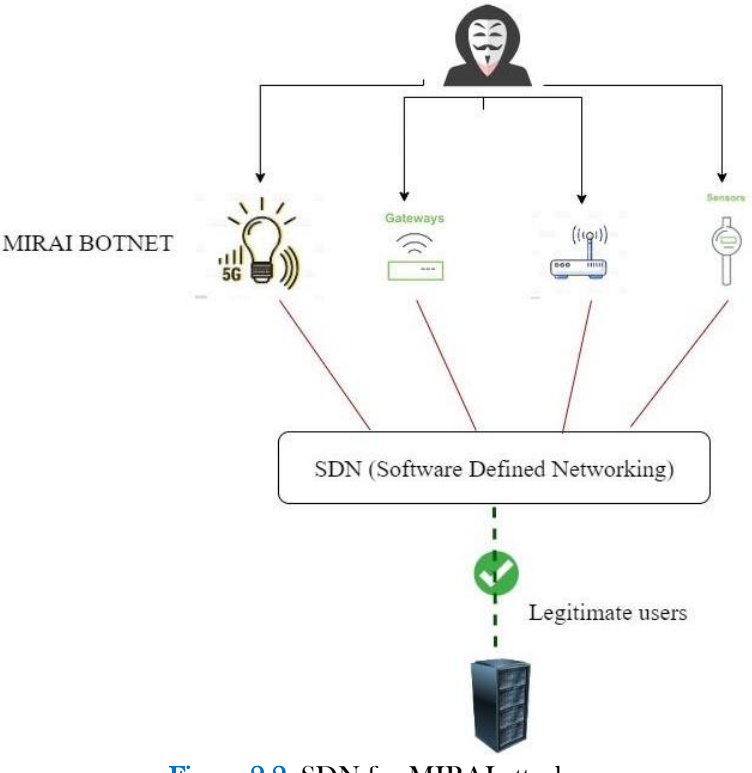

Figure 2.2. SDN for MIRAI attacks

DDoS prevents regular customers from accessing the target network by flooding the network with incoming traffic. Attacks like these are harmful for the organizations. Creating a DDoS attack is simple, detection and solution to attack like these are more challenging. DDoS attacks need to be detected before creating a creator impact, attacks like these lead to EDOS (an economical attack on a network). FCM (Fuzzy C-means Clustering) Algorithm model finds solutions to the aforementioned problems created by DDoS. FCM works by classifying the incoming traffic initiated from BOTNET as clusters. FCM Model works based on the data mining algorithm to detect the attack. The above-mentioned FCM Model can be effective in detecting DDoS attacks in real time [12].

DDoS becomes a major threat to the cloud service providers. The attackers attack by sending vast useless packets to the target IP, aiming to take down the organization. In order to save the organizations or the servers from these attacks, DBSCAN finds a solution to detect the attack precisely. DBSCAN does this work by classifying the useless packets and forming them as clusters. DBSCAN also detects outliers and noise data [13].

Table 2.1 Literature Survey on DDoS

S.No	Authors Details	Techniques Used	Advantages
1.	Reddy et al. 2021	DoS attack detection system using OCSA, CSA, OBL.	Data in the cloud can be protected by detecting the DoS attack using three algorithms.
2.	Gaurav Somani et. al. 2018	Organizations overcome DDoS by following three categories: Attack prevention,detection, and mitigation.	Based on the traffic flow the attacks were classified and segregated by following 3 methods.
3.	Syed Qaiser Ali Shah, 2021	Auto- scaling techniques against ICMP attacks	Dynamic resource utilization (Auto-scaling) safeguards the server from crashing
4.	Niaz Chalabianloo et. al 2017	Software Defined Networking (SDN) to solve IOT based DDoS attacks	SDN solves large scale Mirai based attack
5.	Syed Qaiser Ali Shah et. al. 2022	Mitigating TCP SYN flooding based EDOS attack in cloud computing using binomial distribution in SDN	SYN flooding attacks can be avoided at minimal cost.

3. Proposed Work

The DoS attack mainly targets on the cloud system servers and websites. The AWS platform is affected by DDoS attack by flooding of messages and connection requests. The DDoS (Distributed Denial of Service) drains the cloud resources, so that the users cannot access them. The detection of DDoS attack can be done by using Fuzzy C-means Clustering algorithm. The Fuzzy c-means Clustering algorithm is used to categorize the data points in more than one category. The Fuzzy c-means algorithm is used in detecting the DDoS attack and prevents the AWS system from monetary losses. Fuzzy c-means algorithm works as each data point will be assigned as a member that will be related to cluster center and can be determined by the distance between cluster center and the data points. Fuzzy c-means algorithm falls on soft clustering method.

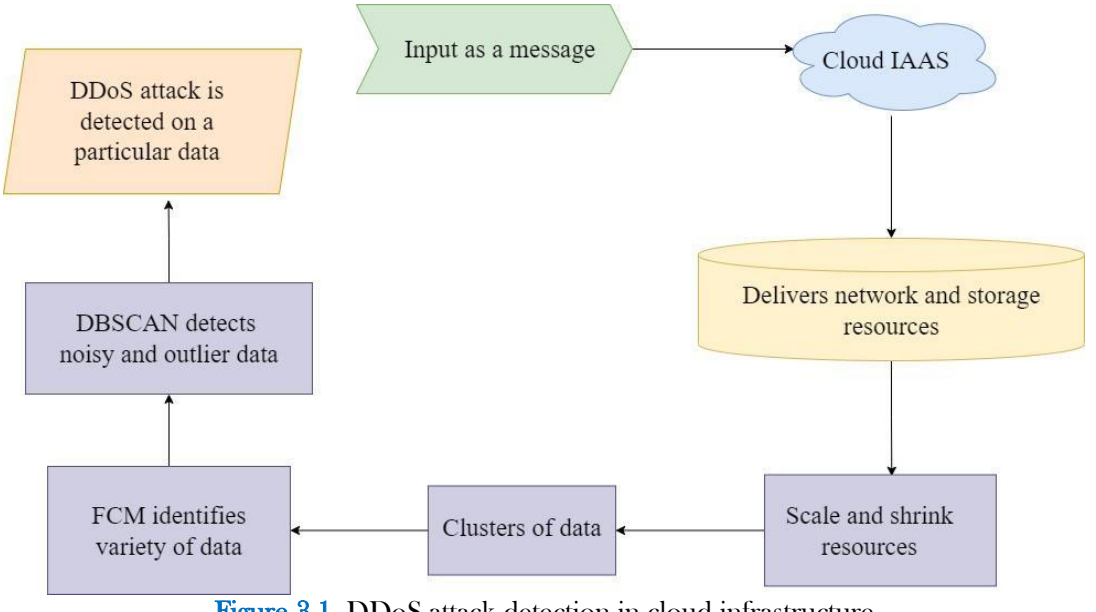

Figure 3.1. DDoS attack detection in cloud infrastructure

The FCM algorithm is used to classify the data into clusters but it cannot detect the outliers. The DBSCAN algorithm helps in outlier Identification and detection of noisy data. Both these algorithms are combined to a hybrid approach where the data can be grouped as clusters and noisy data can be detected. Outliers are the discordant data that are separated from the cluster. Finally, the data are segregated so that the DDoS attack on a particular data in cloud infrastructure can be easily detected. The DDoS attack detection prevents the consumers from losing their message security.

Consider the data, b ∈ D where D is set of elements and **K=** $k_{xy}$where x and y represent the row and column of the fuzzy k matrix that classify data in cloud infrastructure.

Consider **cn** as the noise data (outliers), Initialize **cn=0.**

If the data is found apart from the clusters increment cn=cn+1

The FCM clustering formula that will group the data is as follows,

$$a_{xy}{}^{n} = (\in k_{xy}{}^{n} b_y)^n \,/\, (\in k_{xy}{}^{n}), \forall_y$$

Where a_{xy} is the cluster center, k_{xy} is the fuzzy matrix , b_y) is the input data and **n** is the total no.of data in the cluster.

Let the total no.of datas be t that can be calculated as,

$$t = n+cn$$

The data transmission rate in cloud server can be calculated as,

$$\text{Data transmission rate} = \text{No.of data(t)} / \text{Time} \rightarrow (1)$$

This Data transmission rate will be low when the cloud infrastructure is affected by DDoS attack.

4. Results and Discussion

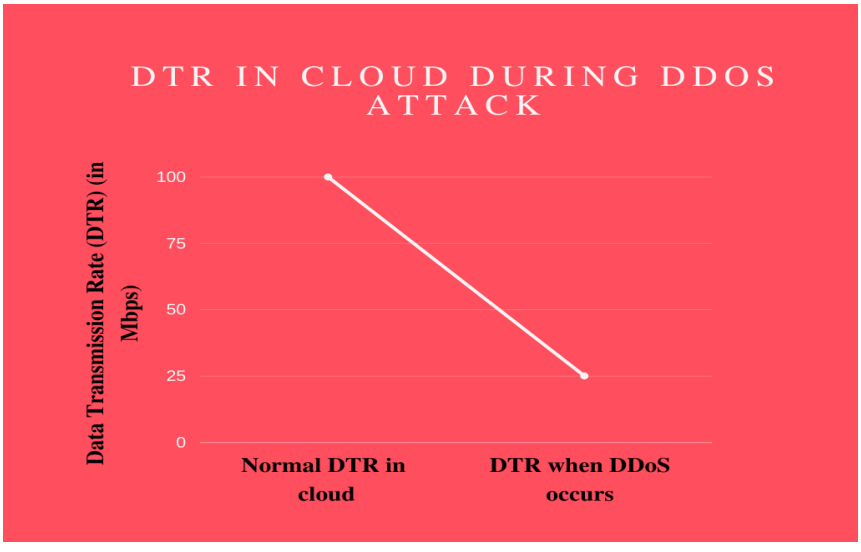

Figure 4.1. Graphical representation of DTR

The above Figure 4.1 displays the variation in Data Transmission Rate(DTR) when the DDoS attack occurs in cloud system infrastructure. This graph is drawn using the formula (1) which determines the DTR. The downfall of the graph tells us that a particular data is affected by the DDoS attack in the cloud system.

The detection rate of DDoS attacks is determined using various algorithms. The Figure 4.2 clearly shows that the new hybrid algorithm that has FCM with DBSCAN displays better detection rate compared to other two algorithms. This hybrid algorithm improves the rate of transmission of data by detecting the DDoS attack precisely.

The Performance of the Algorithm can be determined by using metrics. Consider true positive value as **a** , true negative value as **b** , false positive as **c** and false negative as **d** , then the detection rate of the algorithm can be calculated as follows,

$$\text{Detection rate} = a / a+c$$

Accuracy of the algorithm can be calculated as

$$\text{Accuracy} = a+b / a+b+c+d$$

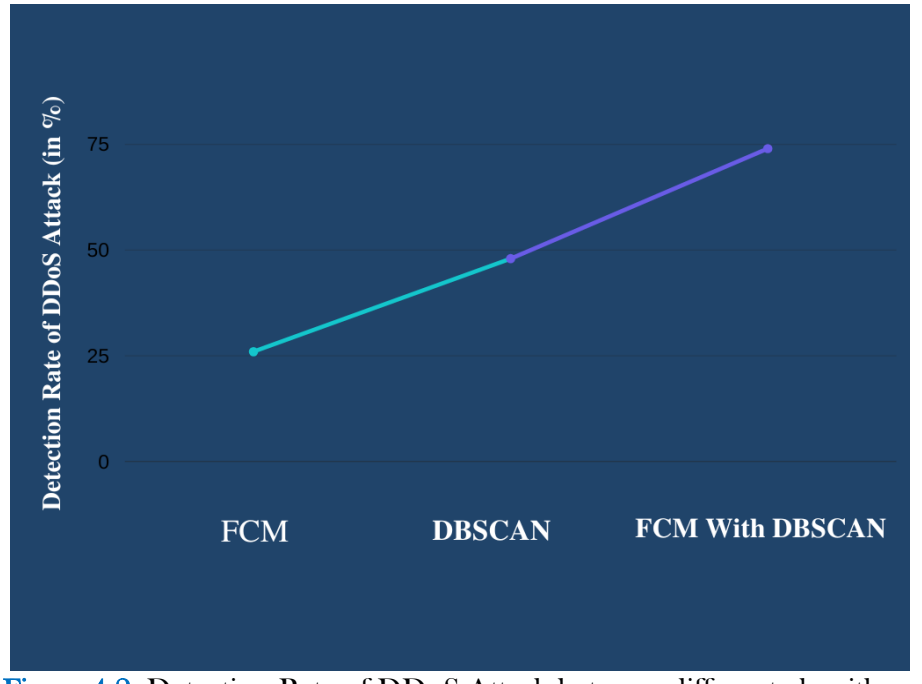

Figure 4.2. Detection Rate of DDoS Attack between different algorithms

5. Conclusion

The DDoS attack targets the cloud system and steals the consumer's security of data with a zombie network. Detecting DDoS attacks is a challenging task for the organization. This paper presents an effective way to detect DDoS attacks at servers over the cloud using Fuzzy c- means clustering algorithm and DBSCAN. The incoming traffic initiated by the attacker contains the noise data and this data can be precisely classified and segregated by following the aforementioned algorithmic models. Finally this detection of DDoS attack improves the Data Transmission Rate and helps the consumers to work comfortably.

References

[1] Devi, T., Priya, J.S., & Deepa, N. (2022). Framework for detecting the patients affected by COVID-19 at early stages using Internet of Things along with Machine Learning approaches with improved Accuracy, *In 2022 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, India. https://doi.org/10.1109/ICCCI54379.2022.9740972

[2] Deepa, N., Priya, J.S., & Devi, T., (2022). Towards applying internet of things and machine learning for the risk prediction of COVID-19 in pandemic situation using Naive Bayes classifier for improving accuracy, *Materials Today: Proceedings*, 62(7), 4795-4799. https://doi.org/10.1016/j.matpr.2022.03.345

[3] Deepa, N., Udayakumar, N., Devi, T., (2022). Management of Traffic in Smart Cities Using Optical Character Recognition for Notifying Users, *International Conference on Computer Communication and Informatics, ICCCI,* IEEE, India. https://doi.org/10.1109/ICCCI54379.2022.9740793

[4] Devi, T., & Deepa, N., (2021). Ant Colony Optimization (ACO) based Improved Edge Detection Algorithm for Segmentation of Brain Tumor, *Annals of the Romanian Society for Cell Biology*, *25*(3), 2849-2867.

[5] Deepa, N., Devi, T., Gayathri, N., & Kumar, S.R., (2022). Decentralized Healthcare Management System Using Blockchain to Secure Sensitive Medical Data for Users, *In Blockchain Security in Cloud Computing,* Springer, Cham. 265-282. https://doi.org/10.1007/978-3-030-70501-5_13

[6] Aravinth, K.P., & Devi, T., (2021). Comparison of Fuzzy-based Cluster Head Selection Algorithm with LEACH Algorithm in Wireless Sensor Networks to Maximize Network Lifetime, *Revista Geintec-Gestao Inovacao E Tecnologias*, 11(4), 1277-1288.

[7] Shah, S.Q.A., Khan, F.Z., & Ahmad, M., (2022). Mitigating TCP SYN flooding based EDOS attack in cloud computing environment using binomial distribution in SDN, *Computer Communications*, 182, 198-211. https://doi.org/10.1016/j.comcom.2021.11.008

[8] Xu, Y., Deng, G., Zhang, T., Qiu, H., & Bao, Y., (2021). Novel denial-of-service attacks against cloud-based multi-robot systems, *Information Sciences*, 576, 329-344. https://doi.org/10.1016/j.ins.2021.06.063

[9] Al-mamory, S.O., & Algelal, Z.M., (2017). A modified DBSCAN clustering algorithm for proactive detection of DDoS attacks, *In 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, IEEE, Iraq. https://doi.org/10.1109/NTICT.2017.7976107

[10] Somani, G., Gaur, M.S., Sanghi, D., Conti, M., & Buyya, R., (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions, *Computer Communications*, 107(15), 30-48. https://doi.org/10.1016/j.comcom.2017.03.010

[11] Özçelik, M., Chalabianloo, N., & Gür, G., (2017). Software-defined edge defense against IoT-based DDoS, *In 2017 IEEE international conference on computer and information technology (CIT)*, IEEE, Finland. https://doi.org/10.1109/CIT.2017.61

[12] Batchu, R.K., & Seetha, H., (2022). On Improving the Performance of DDoS attack detection system, *Microprocessors and Microsystems*, 93, 104571. https://doi.org/10.1016/j.micpro.2022.104571

[13] Al-Mamory, S.O., & Ali, Z.M. (2015). Using dbscan clustering algorithm in detecting ddos attack, *Journal of Babylon University/Pure and Applied Sciences*, *23*(4), 1412-1424.

Funding

No funding was received for conducting this study.

Conflict of interest

The Authors have no conflicts of interest to declare that they are relevant to the content of this article.

About The License