An Effective Distributed Denial Of Service Attack Detection Model In Integration Of Internet Of Things And Cloud Computing Using Binary Fire Fly Optimization Algorithm

E.Helen Parimala, Dr.S. Albert Rabara, P.Theepalakshmi, Y.Sunil Raj

Abstract: one of the serious attacks that occur in the cloud environment is the Denial of Service (DOS) attack that makes the service unavailable for the genuine users. Due to the occurrence of Distributed Denial of Service (DDoS) attack events, it threatens the network security services. Cloud infrastructure is mainly preferred due to the storage of the large datasets. But, this environment faces a serious trouble similar to the Distributed Denial of Service (DDoS) attack that delays the service available to the true users. The attack does not make any trouble happening to the datasets but do affect the resources, services and framework of the cloud. The DDoS attack could be detected by the firewall due to their makeable identity and dynamic nature of attack. A Cloud-based DDOS attack detection model (CDDOSD) had been proposed in this paper that is carried out with the Binary Firefly Optimization Algorithm (BFFOA) and Classification and Decision Tree (CART) classifier. On comparing with the other classification algorithm, CART classifier is found to have the superior learning speed and BFFOA selects the feature from the dataset. The attacks on the cloud host are performed by the tools of the real-time DDoS attack. It is determined that the CDDOSD detects the attack caused by the DDoS with the minimum low false positive rate and promotes high efficiency. BFFOA significantly reduces the feature of the dataset that promotes classification and training with the low dimension of computational space. With the proposed scheme, a secure cloud environment is maintained and also in this paper, the suggested methodology is contrast in the midst of previous mechanism and also establishes to be greater with the performance.

Index Terms: Distributed Denial of Service, Cloud Distributed DOS attack detection (CDDOSD), Binary Firefly Optimization Algorithm (BFFOA), Classification and Regression Tree Classifier CART, Internet of Things.

1. INTRODUCTION

IOT is a paradigm that comes with the two important terms “Internet” and “Things” in the field of information Technology. This novel environment works with the set of interconnected networks through the internet that serves the worldwide users with the Internet Protocol suite (TCP/IP). Through this optical and wireless networking technologies, many public, private, education, business and industrial fields receives their maximum benefits [1]. According to the predictive analyst Cisco and Ericson, The devices connected to through the internet will be increase by the rate of 50 billion by the year 2020. Moreover, this particular estimation had also been revised due to the lack of confidence.

Cloud computing is a huge-scale of distributed computing paradigm. This organized computing service enables in sharing the group of resources to the requested clients through the network. It is not required for the user to purchase any set of software, hardware infrastructure as they are found to be highly expensive. Moreover, the services are provided to the cloud users by the third party. The necessary resources and the service demand could be offered by the third parties to the user based on their pay basis [2]. As per the statement of the NIST at the year 2009, cloud computing is said to be a model that enables a convenient on-demand network access to the communal pool of configurable computing resources, which can be quickly provisioned and released with minimum

effort of management or service provider interaction. Flexibility, pay per usage, maintenance cost, reduced hardware, on demand access and Virtualization are all the factors that tend to make the cloud computing is popular among the users [3]. Many companies tend to adapt cloud computing environment with their infrastructure and it became an advanced technology. Since, internet is the globally accessed connectivity and cloud computing functions through the use of the internet; it tends to become a blooming technology. Recent techniques evolving make the cloud computing services and also the IoT services more advanced. The cloud along with the IoT seeks a new proficiency level in the assigning administration that makes attractive for the IT administration and also business field in expanding their income. Due to their security issues, still the combination of IoT and cloud had not been intended to be used in the larger part of application space and remains in the comprehended writing study. Several challenging highlights attacking the cloud environment is with the lack of security, privacy, QoS, reliability, etc [4]. Attackers also focus on the evolvement of information technology thereby causing severe cyber-attacks day by day [5]. Cloud attack mainly occurs due to the not trustworthy network and plenty of users do the same mistake that affects their privacy. The vulnerability and the attack count had been increased rapidly due to the tremendous users involving with the cloud. Among these severe threats, denial of service (DOS) attack is one among them. Distributed Denial of Service (DDoS) attacks the network server directly and makes the server unavailable for the users [6]. Therefore, DDoS tends degrade the availability for the user. The complete network connectivity will be lost for the user or the victim and the quality will be degraded. The attacker tries to target the

- *Mrs. E. Helen Parimala is currently working as Assistant Professor in Department of Computer Science, M.V.M College, Dindigul, Tamilnadu, India. E-mail: helenandrew07@gmail.com*
- *Dr. S. Albert Rabara is working as Associate Professor in Department of Computer Science, St. Joseph’s College (Autonomous), Tiruchirappalli, Tamilnadu, India. He has 21 years of experience in teaching and 13 years of experience in research. E-mail: a_rabara@yahoo.com*
- *Mrs. P. Theepalakshmi is Research Scholar in Department of Computer Science, National Institute of Technology, Tiruchirappalli, Tamilnadu, India. E-mail: theepalakshmirajan@gmail.com*
- *Mr. Y. Sunil Raj is working as Assistant Professor in Department of Computer Science, St. Joseph’s College (Autonomous), Tiruchirappalli, Tamilnadu, India. E-mail: ysrsjccs@gmail.com*

network and then comprise their agents to launch an attack on the targeted network. DDoS aims in making the resources unable for the victim and the attack mainly tracks the web servers, storage, CPU and other resources. It also damages the virtual serves in the CloudIoT environment thereby reducing the services of the cloud significantly. In the third quarter of 2017, organizations faced an average of 237 DDoS attack attempts per month. Due to the use of IoT, the percentage had been increased to 35% by the second quarter year and by 91% in the first quarter attempt [7]. In the cloud computing environment, DDoS attack is said to be the top nine [8] most threat appearing in this field. Several attack methods had been adapted by DDoS attacks that could be very hard to understand and difficult to defend [9]. According to the researchers, as the usage of cloud increases among the users, the attack could also have a fast growing pace. Additional computational power will be provided by the cloud when the workload increases in order to withstand them. This means that the cloud environment promotes in stopping the threat attack but to the maximum extend the vulnerabilities tries to stop the service by making an attack at every single point before the cloud takes an action [10]. Flooding is the case of the extreme workload faced by the cloud that receives the services from the connected hardware servers. Thus the availability could be affected due to the flooding in which the same service appears to run on the same server. By rising the bill for the usage of the cloud significantly could tend to cause an effect of flooding. Botnet attack [11] is said to be an attack that occurs from the group of computers, one will be assigned as the master and the others will be assigned as slaves by the DDoS attack on the targeted system. Through the botnet attack, DDoS tries to interface many systems and they try to infect all of them, thereby making the attacker unidentified. The best examples of botnet are said to be MyDoom and Trojan. One of the most important attacks of all types is the TCP SYN, in which the target host application will be flooded by the fake ID packets. It is not sufficient to increase the availability of services by increasing the resources since the attackers could attack the target system by adding more computers [12]. Therefore, an effective way to detect the DDoS attack is by implementing CDDOSD based on key feature selection using Binary Firefly optimization Algorithm in the cloud computing environment. Moreover, a comparison result had also been obtained with the other DoS detection algorithm and found that the planned mechanism has more efficiency and minimum rate of false positive. Moreover, the data based on the security of the cloud is not available handy and therefore a private cloud infrastructure is created and the DoS cloud dataset has been created. The next section presents the literature review related to the work that motivates us in pursuing the work in this particular domain. Binary Firefly Optimization Algorithm with their modifications for the feature selection had been presented in Section 3. The CART Decision Tree Classifier is described in Section 4. The next section is carried out by the outline of the proposed scheme and the experimental results had been shown in the Section 6 followed by the conclusion.

2 REVIEW OF LITERATURE

Several researches had been done in the DDOS attack detection in the cloud that is available in several articles. Few of these papers are talked about in this segment. A protocol projected for the enhancement for the secure cloud had been presented in [13], which follows a cost effective method for authenticating the cloud user securely and also prevents the internal and the external DoS attacks. This protocol is said to be a lightweight protocol as they utilize the minimum resources of cloud. But the main drawback of this model is that it could only be used with the layer of SaaS. Later, a protocol known as the Enhanced Cloud-Based Secure Authentication had been developed working in both the IaaS and the PaaS layer. Considering the price factor, [14] described a low rate DDoS attack that could detect the malware earlier thereby gaining the cost value. A ping-of-death attack had been proposed by [15], where byte size of about 65,536 will be contained in the ping packet. Later, this value increases to IPv4 packet size. Due to the buffer overflow, these packets could be crashed or it should be rebooted with the later evolved operating systems. Transmission Control Protocol (TCP) lies on the top of the transport layer of the TCP/IP model stack, which is said to be the connection oriented protocol. This connection could be established by three-way handshaking mechanism prior to the packet transmission among the client and the server. A SYNC message will be sent by the connecting host during the transmission, in return which has to receive the SYN + ACK message sent by the remote host. This handshaking process could be complete once the final ACK is responded by the connecting host and then the connection could be done among the client and the server. This connection could be suppressed by the attackers by making a half-opened connection that creates several transmission lock allocation and also drain out the kernel memory [16]. This could be completed by carrying out the coordinated task through the vulnerable nodes filtration from the internet. With the spoofed IP address, TCP SYN flooding with DDoS attack could be made possible. During this attack, the host will not receive the final ACK message sent to establish the connection and the spoofed IP carrying host will react to the RST flag (or it could be said that the host will not be present). Cha et al [17] presented a paper regarding the TCP SYNC flooding attacking that had occurred in the Amazon cloud services. Moreover, in [18] the author had tested and measured the service quality of the cloud environment. In this paper, the author had also estimated the efficiency after the establishment of cloud server. While testing the function of the cloud server, the average throughput value was determined to be 45.438 Mbit/s before the attack of DoS and reduced to 35.863 Mbit/s after the attack of DoS. This made a clear view that the DoS attack could possibly reduce the throughput of the system. The current host's connectivity status could be known by the ICMP, which is said to be an IP protocol. This ICMP could be used by the attackers in the form of smurf and ping flood attacks, in order to launch a DoS attack in the cloud server. Several ICMP packets will be directed that targets in consuming the bandwidth and also crashing the target system. Finally, the target will not respond to the user for any incoming request as a result. A new method to avoid the DDoS attack had been given by [19]. When an attack occurs then the appropriate preventive measure is necessarily taken so that this could not result in immediate failure at the future. The true positive rate (TPR) value will become 0.85 when a new attack is launched and the value will be 0.072 during the False Positive Rate (FPR). The reduction in accuracy at intermediate points will be 0.70. Smart guideline based attack discovery had been

proposed in [20] for the cloud environment. This was based on the host properties and during the detection of any attacks some threshold will be created. For classification of the attacks, the manual element choice had picked just 30 highlights out of 47. For 10,000 records and ten times cross approval, the accuracy for the classification of the proposed system is determined to be 98.46%. With certain other feature selection methods this model could be enhanced. Based on the Clustering, Classification and with certain threshold value DoS attack could be determined in the cloud computing. Based on the dataset used, the accuracy could be determined. The attack detection could not be perfect only with the firewall, since many new attacks had been evolving (Identity masking in the botnet attack) with the advancement in cloud features. The dataset available in the internet could lead to legitimate activity and heavy traffic. Traffic could also increase due to the heavy competition. Therefore, DoS attack could not detected only by measuring the traffic. The host properties could also be utilized for detecting the DDoS attack, which had been presented in this paper. Moreover, the host value could change based on the DDoS attack. The DoS attack could be detected by the significant model of the cloud host resources. Any deviation at this point could lead to DDoS attack. A cloud denial of service attack detection model with the technique of key feature selection with the novice binary version of artificial bee colony optimization and decision tree classifier had been implemented in [21]. This paper does not involve in detecting multiple threats and also network properties could be implemented in this paper, which is found to be a drawback. In this situation, detecting several threats could be done by determining several attributes.

3 BINARY FIREFLY OPTIMIZATION ALGORITHM

A recently developed metaheuristic known as the Binary Fire Fly Optimization Algorithm (BFFOA) had been developed. This had been proposed by [22] with the inspiration occurred from the fireflies producing flash lights. This stochastic meta-heuristic algorithm involves in solving many complex optimization problems and certain NP-based problems that includes traveling salesman problem, quadratic assignment problem [23], graph scheduling problem [24], and job shop scheduling problem. A survey based on the Firefly Algorithm had been done in [25]. According to this algorithm, the brighter the firefly the more it attracts the other and this concept had been utilized in obtaining the objective solution. There will be an exponential decrease with the brightness of the light as the flies moves to the further distance due to the light absorption by the medium. BFFOA has the following assumption [26]: The fireflies get attracted to one firefly regardless of their sex as they are unisex in nature. Brightness will be the main important factor for the firefly to get attracted. This brilliance will be contrarily corresponding to the separation. If the brightness of the firefly lowers then the others will be in the search of the new brighter one. The firefly brightness determines the landscape of the objective function. The simplified equation based on the distance among the two fireflies (i and j) at xi and xj, respectively, could be given by the Euclidean distance equation as, Eq 1

$$r_{ij} = \| x_i - x_j \| = \sqrt{\sum_{k=1}^{d} (x_{i,k} - x_{j,k})^2} \quad \text{Eq1}$$

Where, k=1.

As said earlier, the attractiveness of the fireflies decreases with the increase in the distance. This distance of attractiveness r is given by,

$$\beta(r) = \beta_0 e^{-\gamma r m}, \; m \geq 1. \quad \text{Eq 2}$$

Here γ -light absorption coefficient;

β_0 – attractiveness at distance r = 0, usually accepted as one;

and m-Exponential curve sharpness usually taken as m=2.

For a given length scale Γ in an optimization problem, Γ−m is used as the initial value for γ. The firefly i gets attracted to the other firefly j, which is defined by the equation as,

$$X_i = X_i + \beta(rij)(X_j - X_i) + \alpha(\varepsilon - 0.5). \quad \text{Eq3}$$

Here ε is a random number drawing from standard uniform distribution (i.e. $\varepsilon \sim U(0,1)$); and $\alpha \in [0,1]$ is the scaling factor of the randomness.

Algorithm 1: BFFOA

Initialize variables for BFFOA;
initialize populace for fireflies;
assess firefly populace;
computerize the light power Ii;
while V < Best do
for x= 1 : m (all m fireflies) do
for y= 1 : m do
if Ij > Ii then
firefly x position travel close to firefly y position;
end
engaging quality changes dependence on separation;
add assessment new arrangement;
revise the light force Ii;
end
end
qualities based fireflies and select best firefly;
revise worldwide best whenever required;
if execution paradigm fulfilled then
finish assess process;
end
end

return the worldwide best feature; Several researchers had carried out the work based on the Firefly algorithm to solve the continuous optimization problem. For encrypting the message from the cryptanalysis, binary firefly algorithm had been used in [27] for deducing the meaning from the message. Only limited amount of study had been carried out with the integer programming problem. For the distributed and parallel systems, the binary adaptive Firefly Algorithm had been implemented in [28] in order to identify faults or malware in the system. Binary real coded Firefly Algorithm had been used in [29] for resolving the problem committed by the set of connections and trustworthiness controlled unit. In all these studied the continuous variable had been transformed to the binary variables through the sigmoid function and also measure of light intensity is done by Euclidean distance.

A. Character building of firefly

Each firefly is represented in terms of n binary digits (n string bits). The feasible solution is represented as a bit string $\vec{x} \in \{0,1\}n$. Diversification from the population could be attained by selection of initial populating randomly from all dimensions. The criteria will be stopped once the following criterion is attained: 1) Reach maximum iterations 2) attaining the optimal solution 3) repeated iterations that could not be improved

further and 4) attaining the maximum run-time. If the solution reaches any of the following criteria then the algorithm terminates.

B. Remoteness of two fireflies

Hamming distance is defined as the distance among the two fire flies i and j i.e., number of elements present between their permutations. The difference in the values of the objective function will be proportional to the Hamming distance.

1) Enchantment of fireflies: If the objective function value of i is smaller than j then it means that the attraction among them will be greater. This attractiveness is given by the formula

A firefly i attracted to another firefly j, if the objective function value of i is smaller than the objective function value of j. The attractiveness of firefly i with respect to firefly j is given by the equation,

$$\beta(rij)= \beta_0 e^{-\gamma r2ij} \quad \text{Eq4}$$

Where,

rij - the Hamming's distance among the fireflies i and j.

γ is the light absorption coefficient and these values varies between $\gamma \in [0,\infty]$, here γ is considered among the range of [0.01,0.20].

C. Motion of fireflies:

The movement of the fireflies in the continuous problem is defined by the following equation

$$X_i =(1-\beta(rij))X_i +\beta(rij)x_j \quad \text{Eq 5a}$$

$$X_i =X_i +\alpha(\mathcal{E}-0.5). \quad \text{Eq 5b}$$

The following steps will be followed by the firefly while moving within the solution space: The movement of the firefly i to the other one j will be determined by β (rij) in the first step (given in equation 5a). The random movement is defined by α, which is defined as the next step (given in equation 5b). These two steps should not be interchanged. β –step is the first step and from the above equation it is known that xi will be equal to xj with the probability β (rij); (1−β (rij)) is the probability for the xi to be unchanged. Next, the α value will be chosen from the range [0,1] and for the continuous optimization problem the movement of the firefly will be chosen at the random. The xi will require a large step if the value of α is very high that leads to the lag of the current solution. On the other hand, α value is low means the new arrangement acquired will be inside the little neighborhood of the present solution. The global and local search value is determined by α and the balance could be maintained by this exact search procedure. But determining the value of α is not an easy job. The α –step represents the modification in the bit values from the binary set of the fireflies. The bit values from the binary set could be changed in the following ways: 1) Swap procedure 2) Flip procedure. The change in the value of bits (nB) will be based on the Hamming distance (i.e., rij) since the distance among the fireflies i and j should be significantly reduced and this could be based on the brightness of the firefly. If the firefly xj is brighter than firefly xi then xi attracts towards xj. Therefore, nB=α × rij as well as α should be minimum. Else, the Hamming distance will be increasing rather than decreasing. This is analogous to variable distance move(k-distance or k-exchange) and the value of k is chosen as 1.

4 CART (DECISION TREE CLASSIFIER)

CART commonly known as Decision tree Classifier, these classifiers work on the principle of learning from the group of labeled data instances, which can successfully classify the test instances under any classes. CART consists of two vital stages, training stage and testing stage. In the training stage, the CART classifier employs existing training data labels as well as characteristics for the purpose of learning and in the testing stage, the CART classifier produces the classification output of a test instance which maybe anomalous or normal. During the path of each repetition of the bonanza, the correctness of the CART classifier and its importance features which can aggrandize the classifier are recorded. Subsequently, the bonanza is able to produce the optimal feature subset known as BFS which records the best and effective accuracy.

5 PROPOSED CDDOSD AND BFFO MODEL

By employing Apache Cloudstack [31], the DOS cloud dataset is extracted and experimented by using a private cloud. In the private cloud, ten interconnected computers are chosen and suitable computer which has higher memory capacity and processor speed is selected as the cloud host machine. In-order to create a private cloud environment, Apache cloud stack was installed on the host and host machine comes with 3.2 GHz of CPU, 16 GB of RAM as well as 1 TB of hard disk. The behavior, characteristic as well as performance are monitored during the DDoS attack. A real-time DDoS attack is carried out on the cloud host machine, the tools employed for performing a real-time DDoS attack are LOIC(Low orbit Ion Canon),XOIC, DDoSIM, PyLoris, Hulk. As soon as the attacks commences, there were modifications in the performance of the cloud host assets, namely, network, CPU, memory storage as well as socket values, these modifications led to under performance of the cloud host machine. By employing various attack tools at different intervals, ten connected computers attacked on the targeted cloud host. The attackers are disguised as normal users during the DDoS attack in which ten computers are employed for this purpose. More than 20,000 instances are gathered, out of which 10000 instances are normal cloud usage pattern. A DDoS cloud data set was created and its features of the cloud host along with DDOS attack detection as shown in figure 1. The highlights of the cloud have that are discovered helpful by perception in DDoS assault identification are recorded in the Dos cloud dataset and their clarification are given in Table 1. In-order to lessen the computing space as well as enhance faster response, feature extracting technique plays an important role in enhancing prevention tools against DDoS attack. By integrating CART with BFFOA, the proposed technique successfully detects DDOS attack. As the first stage, properties of the host are extracts so that DOS cloud dataset can be created. In CDDOSD, the BFFOA chooses a feature subset existing in the DOS cloud dataset and with 80 % training is allocated to the CART classifier in the training stage and 20% for testing the records of chosen feature subset during the iteration of the algorithm.

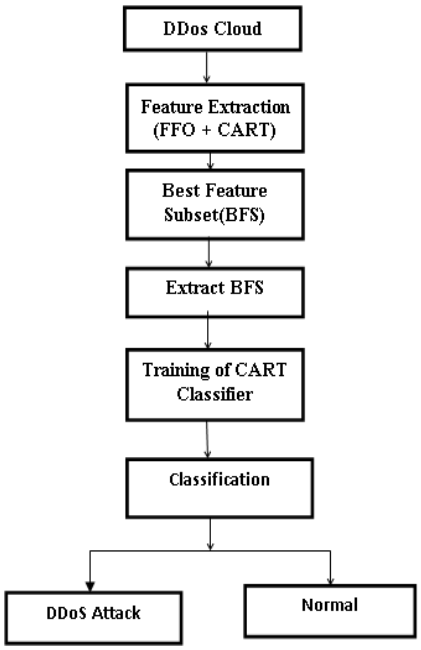

Fig 1. *Proposed CDDOSD MODEL*

During each iteration, accuracy of the classifier and its chosen feature subset are monitored. The optimal accuracy based on the corresponding feature subsets are determined and this feature subset is considered as optimal feature subset known as BFS.

TABLE 1
DDoS CLOUD DATASET PROPERTIES

S. No	Cloud Premises	Explanation
1	full Cpu , sys	running system processes, idle, waiting.
2	Disk/Total, read	Total no of read or write operations in disk.
3	Paging, in	copied or moved to memory.
4	Load Avg , 1M	The average load of Cpu performance in 1M, 5M
5	free	buffered, cache memory usage.
6	Network, sent	The quantity of bytes, sent or received on the system interface.
7	Processor, new	No of process running, blocked, newly created.
8	Io/Total, Write(io)	No of read and write request in system call.
9	Swap, used	not in use.
10	Sockets, TCP	No of TCP connection established, no of TCP sockets in use.

In-order to lessen the computing space as well as enhance faster response, feature extracting technique plays an important role in enhancing prevention tools against DDoS attack. By integrating CART with BFFOA, the proposed technique successfully detects DDOS attack. As the first stage, properties of the host are extracts so that DOS cloud dataset can be created. In CDDOSD, the BFFOA chooses a feature subset existing in the DOS cloud dataset and with 80 % training is allocated to the CART classifier in the training stage and 20% for testing the records of chosen feature subset during the repetition of the algorithm. During each iteration, efficiency of the classifier and its chosen feature subset are monitored. The optimal accuracy based on the corresponding feature subsets is determined and this characteristic division is considered as optimal feature subset known as BFS.

5.1. CDDOSD Proposed Algorithm

1. Each feature x_m is initialized by using equation (1)

$$r_{ij} = \| x_i - x_j \| = \sqrt{\sum_{k=1}^{d} (x_{i,k} - x_{j,k})^2} \quad \text{Eq 1}$$

2. $X_{md}=l_i+rand(0,1)*(u_i-l_i)$ where d = 1, 2, …, D; is the list of the characteristic in firefly location foundation vector, ui and li are the higher and minor bounce of i^{th} parameter of the problem
3. Initialize the firefly location matrix using equation. (1)
4. Convert this firefly location matrix into binary values eq(2,3)
5. $\beta(r)= \beta_0 e^{- \gamma r m, m>} m \geq 1$ Eq 2
6. $X_i = X_i + \beta(rij)(X_j - x_i) + \alpha(\mathcal{E}-0.5)$ Eq 3
7. While(true)
8. suggest feature division to the CART classifier
9. guide and assessment the CART classifier and find the categorization accurateness based on fitness value.
10. // Calculate the brightness feature value for the firefly
11. //Calculate the fitness value for the every firefly
12. Convert the brighter firefly for the less attractive firefly location using equ4
13. $\beta(rij)= \beta_0 e^{- \gamma r 2ij}$ Eq4
14. suggest the feature division selected by firefly brighter location cause to the CART classifier
15. train and test the CART classifier and find the accuracy(fitness) of classification
16. for i=1 to no of feature
17. for j=1 to no of feature
18. if(fitness(of i^{th} firefly > fitness of j^{th} firefly)
19. i^{th} firefly move towards to the j^{th} firefly
20. if(fitness value of i^{th} feature of the fitness value)
21. // i^{th} feature move towards to the j^{th} feature depends upon the fitness value
22. end if
20. end for
29. end for
30. find out the best fitness among all the fireflies.
31. The Best firefly based on fitness value move randomly
32. If random moveness gives the best fitness than replace it.
33. If more than 10,000 iteration no improvement is there to select best fitness firefly
34. Break
35. end while

In CDDOSD Algorithm, Firefly area initialized randomly in step1 in real values. The firefly location formed for the duration of course of the bonanza are changed real values into binary numbers by using eq 2,3. The CDDOSD utilizes the firefly area for highlight determination utilizing BFFOA. The highlights in succession of firefly area source grid relates to the worth 1 are chosen and 0 are not chosen for preparing and assessment of CART Classifier. The exactness of the classifier and the chosen highlight subset are recorded in stage 30. In each cycle of the bonanza, the new firefly areas are establish in step 3 and the feature division of new firefly areas are chosen and functional in the training and estimate of CART Classifier. The fitness estimation of firefly is estimated for new firefly areas. Fitness worth dependent on ith firefly more prominent than jth firefly. On the off chance that the arrangement exactness is discovered superior to anything the old firefly area is supplanted by new firefly area in stage 16. Generally the new firefly areas are abandoned in stage 7 after a characterized trail limit. In addition in excess of 10000 emphases no improvement for giving best fitness firefly then the procedure are abandoned.

6 EXPERIMENTAL SETUP

Apache Cloud Stack is installed on ten computer systems which acts as a private cloud. The computer machine consists of Intel i5 processor with an impressive processor speed of 3.20 GHz with its memory capacity of 16 GB RAM. When DDoS attack occurs, the Linux as well as Window based virtual devices are monitored and recorded on the cloud host which uses Ubuntu as the cloud host operating system. The reason for employing Ubuntu as the cloud host operating system is that it provides effective security. The installed Apache Cloud Stack is configured such a way that it can provide private cloud environment. The properties of the host are monitored even later then the DDoS attack. By employing real-time DoS attack tools, five devices are accessed by the virtual machines on the cloud host and remaining five machines are used to carry out the attack on cloud host. Generally, DDOS attacks starts its process by deploying traffic on large scale on targeted cloud host, thereby interrupting the cloud computing services to its legitimate cloud users. The traffic creates havoc by using the cloud host resources to its maximum potential. However, the CDDOSD detect these attacks by observing the resource usage pattern which leads to successful identification whether a DDoS attack is taking place or not since most DDoS attacks are not, detected at the beginning of the cloud host machine, CDDOSD chooses the BFS from DOS cloud dataset by employing BFFO. By employing ten cross validation, the performance of the CDDOSD is determined which is trained and test in the ratio of 80:20 ratio which consists of 40,000 records of DOS cloud dataset. As shown in table 2, BFS and its performance of proposed technique is recorded. The experimentation results are done by employing MATLAB. The cloud data set consists of DDoS attacks. In-order to determine the performance of CDDOSD, F1-Score as well as false positive rate measures is employed. Accuracy is provided in the Eq. (1) in which high accuracy is achieved,

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \qquad \text{Eq 1}$$

Here,

TP (True Positive) presents attacked samples

TN (True Negative) presents normal attacked samples.

FP (False Positive) presents the number of samples which are usual and classified as assault;

FN (False Negative) presents the number of samples which are assault and classified as usual.

TABLE 2
CLOUD DATA SET FOR COMPARISON

Model	No of Selected Features	Method	Accuracy %	FPR %	F1 Score
CDDOSD	10	80% training, 20% testing dataset	98.24	0.0002	98.4
		tenfold cross validation	98.34	0.0002	98.34

BFS contains 10 features selected by BFFO

BFS: sys, read (disk/total), in, 1M, free, send, New, write(io), used (swap), tcp.

As present in the table 2, the proposed technique provides optimal classification accuracy as well as low false optimistic rate is observed when the features are chosen by BFFOA employing tenfold cross justification in which classification efficiency of 98.34% and low false positive rate of 0.0002 is achieved when compared with traditional detection techniques. Pradeepthi [32] proposed a smart rule-based feature selection as well as classification method which can successfully detect DOS attack. The authors have employed dataset with 47 attributes as well as chosen 30 attributes. Table 3 shows that accuracy has been achieved up to 88.46%. Seth has proposed DoS Attack Detection through Abc colony optimization. Having utilized dataset with 30 characteristics and chose 12 credits to choose assault. The exactness of the model is recorded as 92.79%. The general correlation of proposed CDDOSD model with other existing identification models are appeared in Table 3.

TABLE 3
PERFORMANCE COMPARISON OF CDDOSD & BFFO WITH OTHER EXISTING FINDING MODELS

Detection Model	Number of Selected Features	Accuracy (%)	False Positive Rate
IRCM - Intelligent rule based classification model	30	88.46	0.008
BABCO -DOS using CART and BABCO	12	92.79	0.004
CDDOSD & BFFO-Proposed CDDOSD using CART and BFFO	10	98.34	0.002

Proposed model compared with other detection model is depicted in figure 2. The proposed models have high accuracy

98.34% and also false positive rate is reduced as 0.002 compared with other detection models.

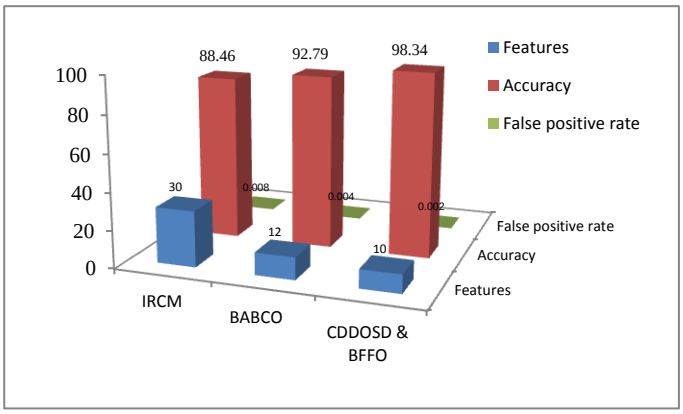

***Fig 2** PROPOSED CDDOSD & BFFO*

7 CONCLUSION

The collection of the data set from the monitored cloud host can easily detect DDOS attack and most properties of the cloud host machine varies, therefore the properties of the host are observed and the proposed technique can detect DDOS attack. The proposed CDDOSD model with BFFOA highlight choice improved the discovery exactness and has a low false positive rate. The decrease of the highlights from DoS cloud dataset makes the proposed model progressively proficient.

REFERENCES

[1] Islam S, R Kwak, D Kabir, H Hossain, M Kwak,, "The Internet of Things for Health Care: A Comprehensive Survey", Access, IEEE, 3, 678–708, 2015.

[2] Kumar U, Gohil B.N, "A survey on intrusion detection systems for cloud computing environment", International Journal of Computer Application. 2017, Doi: 10.1016 / j. jnca . 2016 .10. 015.

[3] P. Mell and Grane, "The NIST definition of cloud computing," NIST special publication, vol 800, no.145, 2011.

[4] S. Sivakumar, V. Anuratha, S. Gunasekaran, "Survey on Integration of Cloud Computing and Internet of Things Using Application Perspective," International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359 (Volume-6, Issue-4). April 2017.

[5] M. Waterhouse, "Rutgers University's computer network under DDoS attack", http: // abc7ny.com/technology/rutgerscomputer-network-underattack,website-internet-access-down-on campus/1006255, 2015.

[6] Rashmiv Deshmukh, Kailas K.Devadkar, "Understanding DDoS Attack & Its Effect In Cloud Environment," Elsevier, doi:10.1016/j.procs.2015.04.24.

[7] Akamai, "State of the internet security", Q3 2017 report, 2017.

[8] The Notorious Nine, "Cloud Computing Top Threats in 2013", http://downloads.Cloudsecurityalliance.org/initiatives/topthreats/TheNotoriousNineCloudCompuitngTopThreatsin2013.pdf.

[9] RashmiD, Kailas D, "Mitigating ddos attack in cloud environment with packet filtering using iptables", International journal of Computer Engineering and Applications, volume VII, Issue II, August 14.

[10] Meiko Jensen, JorgSchwenk, Nil Crusehka, "On technical issues in cloud computing", IEEE International Conference on cloud Computing, 2009.

[11] Deshmukh R. V Devadkar, K. K. (2015),"Understanding DDoS attack and its effect in cloud environment". In Procedia computer science (Vol. 49, pp. 202–210).https: //doi. Org /10.1016 / j.procs. 2015.04.245.

[12] Xiao, L., Wei, W., Yang, W., Shen, Y., & Wu, X. (2017). A protocol-free detection against cloud oriented reflection DoS attacks. Soft Computing, 21(13), 3713–3721. doi.org/10.1007/s00500-015-2025-6.

[13] Darwish M., Ouda, A,(2017),"An enhanced cloud-based secure authentication (ECSA) protocol suite for prevention of denial-of-service (DoS) attacks", International Journal on Future Revolution in Computer Science & Communication Engineering, 3(11), 485–496.

[14] M. Ficco, and M. Rak, "Stealthy denial of service strategy in cloud computing", IEEE Transactions on Cloud Computing, 3(1) (2015) 80-94.

[15] Balobaid A, Alawad, W Aljasim, H. (2016). A study on the impacts of DoS and DDoS attacks on cloud and mitigation techniques. In International conference on computing, analytics and security trends, CAST 2016 (pp. 416–421), https://doi.org/10.1109/cast.2016.7915005.

[16] F. Wong, C.X. Tan, "A survey of trends in massive DDoS attacks and cloud-based mitigations", International Journal of Network Security & Its Applications (IJNSA) 6(3), 2014, 57-71.

[17] B. Cha, J. Kim, "Study of multistage anomaly detection for secured cloud computing resources in future internet". In: Proceedings of IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, Australia, 2011, pp. 1046-1050.

[18] Bahaweres, R. B., Sharif, J., Alaydrus, M,"Building a private cloud computing and the analysis against DoS (denial of service) attacks: Case study at SMKN 6Jakarta". In Proceedings of 2016 4th international conference on cyber and IT service management, CITSM 2016. https://doi.org/10.1109/citsm.2016.7577583.

[19] Vidal, J. M., Orozco, A. L. S., Villalba, L. J. G, Adaptive artificial immune networks for mitigating DoS flooding attacks. Swarm and Evolutionary Computation, 38, 94–108.

[20] Pradeepthi, K. V., Kannan, A, (2015)," Cloud attack detection with intelligent rules". KSII Transactions on Internet and Information Systems, 9(10), 4204–4222.

[21] Jitendra Kumar Seth, Satish Chandra, "An effective DOS attack detection model in cloud using Artificial Bee Colony Optimization", springer, 2018, https://doi.org/10.1007/s13319-018-0195-6.

[22] X. Yang, "Firefly algorithm", Nature-Inspired Metaheuristic Algorithms, vol. 20, pp. 79–90, 2008.

[23] U. Honig, "A firefly algorithm-based approach for scheduling task graphs in homogeneous systems," in Informatics. ACTA Press, 2010, pp. 24–33.

[24] K. Durkota, "Implementation of a discrete firefly algorithm for the qap problem within the seage framework,"

Master's thesis, Electrical Engineering, Czech Technical University, Prague, 2011.
[25] I. Fister, I. Fister Jr., X.-S. Yang, and J. Brest, "A comprehensive review of firefly algorithm," Swarm and Evolutionary Computation, vol. 13, pp. 34–46, 2013.
[26] X.-S. Yang, "Firefly algorithm for multimodal optimization," Lecture Notes in Computer Science, vol. 5792, pp. 169–178, 2009.
[27] S. Palit, S. Sinha, M. Molla, A. Khanra, and M. Kule, "A crypto analytic attack on the knapsack crypto system using binary firefly algorithm," in The Second International Conference on Computer and Communication Technology, ICCCT-2011, IEEE,2011, pp. 428–432.
[28] R. Falcon, M. Almeida, and A. Nayak, "Fault identification with binary adaptive fireflies in parallel and distributed systems," in IEEE Congress on Evolutionary Computation, CEC-2011, IEEE,2011, pp. 1359–1366.
[29] Chandrasekaran and Simon,"A binary firefly algorithm for knapsack problems", 2015, 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), DOI: 10.1109/IEEM.2015.7385611.https://cloudstack.apache.org.
[30] DDoS attack tool timeline, http://staff. washington.edu/ dittrich/ talks/ sec2000/timeline.html.
[31] Pradeepthi, K. V., Kannan, A, (2015), "Cloud attack detection with intelligent rules. KSII Transactions on Internet and Information Systems", 9(10), 4204 – 4222.https://doi.org/10.3837/ tiis.2015.10.025.