ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Intrusion Detection System Using SVM Classifier for Detecting DoS Attack in Cloud Platform

Kirti Ramhariya[1], Prof. Satpal Singh[2]

M.Tech. Student, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[2]

ABSTRACT: Network firewalls act because the initial line of defence against unwanted and malicious traffic targeting net servers. Predicting the firewall performance is crucial to network security engineers and designers in assessing the effectiveness and resiliency of network firewalls against DDoS (Distributed Denial of Service) attacks as those normally launched by today's Botnets. Distributed Denial-of-Service attack (DDoS) may be a major threat for cloud atmosphere. ancient defensive approaches can not be simply applied in cloud security because of their comparatively low potency, giant storage, to call some. Distributed denial of service (DDoS) attacks is that the second most rife crime attacks when info thieving. DDoS TCP flood attacks will exhaust the cloud's resources, consume most of its information measure, and injury a complete cloud project at intervals a brief amount of your time. The timely detection and interference of such attacks in cloud comes are so very important. The projected system offers an answer to securing the system by real time packet observation and keep records by classifying the incoming packets and creating a choice supported the classification results. throughout the detection section, the system identifies associate degreed determines whether or not a packet is traditional or originates from an assaulter. throughout the interference section, packets, that are classified as malicious, are denied to access the cloud service and also the supply information processing will be blacklisted. The virtualization for cloud, packet instrument Wireshark and support vector machine (SVM) is employed to implement the projected system. The performance of the projected system is compared victimisation the various existing systems with differing types of classification and packet filtering and analyzing techniques like OSSEC. The results show that projected system yields the simplest performance with changed classification and packet filtering technique in real time with improved potency.

KEYWORDS: DDoS Attack, Cloud, Virtualization, SVM, Wireshark, IP Packets, OSSEC

I. INTRODUCTION

Distributed Denial-of-service (DDoS) assault may also be viewed as a predominant threat to cloud computing. The attackers in general compromise vulnerable hosts, known as zombies, on the community and set up attack tools on them. These zombies collectively type a botnet and will generate huge quantity of distributed attack packets focusing on at the victims under the manipulate of the attackers. This assault will block the respectable entry to the servers, exhaust their assets such as network bandwidth, computing vigor and even lead to pleasant monetary losses as proven in [3]. Firewalls themselves may also be subjected to malicious attacks from the internet as they're probably deployed at the fringe of the community.

One of the severe assaults is the disbursed Denial of Service (DDoS) attack. If network firewalls are poorly designed to withstand DDoS attacks, the total safety of the included community will probably be jeopardized. In particular, there's

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

an growing demand for analytical models to support firewall designers in predicting how potent and efficient is the network firewall under DDoS assaults. Additionally, modelling and analyzing the performance of community firewalls can be extremely priceless in gaining a deeper working out of firewalls' habits and characteristics. Firewall designers and procedure administrators can establish bottlenecks and key parameters that impact its performance, and then perform the integral tuning for top of the line efficiency. Analysis can furnish rapid answers to countless design and operational questions. For illustration, firewall designers can use evaluation to hold out a first reduce design to lower the set of design possible choices and then use simulations and/or experiments to assess few excellent designs earlier than constructing and deploying the method. Distributed Denial of Services (DDoS) TCP food attacks are DoS attacks where attackers food a victim laptop with packets to be able to exhaust its resources or eat bandwidth [1]. As the attack is also distributed over more than one machine, it'll be very hard to distinguish professional users from attackers. In fact, a DDoS ood assault will not be handiest a popular attack; it is the 2nd most fashioned cybercrime attack to motive financial losses.

1.1 DOS ATTACK

Denial of provider (DoS) assault often called TCP SYN Flooding. The attack exploits an implementation attribute of the Transmission manipulate Protocol (TCP), and can be utilized to make server techniques incapable of answering a authentic consumer application's requests for brand new TCP connections. Any carrier that binds to and listens on a TCP socket is possibly vulnerable to TCP SYN flooding assaults. On account that this includes well-known server purposes for email, internet, and file storage services, working out and realizing tips on how to defend towards these attacks is a significant part of realistic network engineering [12]. The basis of the SYN flooding attack lays within the design of the 3-manner handshake that starts off evolved a TCP connection. On this handshake, the third packet verifies the initiator's potential to obtain packets on the IP handle it used as the source in its initial request, or its return reach ability. Figure shows the sequence of packets exchanged on the establishing of a average TCP connection.

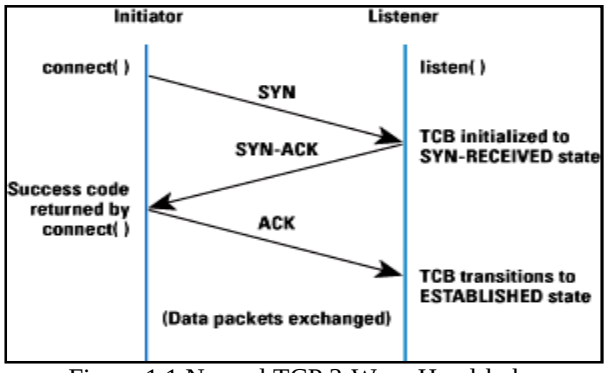


Figure 1.1 Normal TCP 3-Ways Handshake

The Transmission manage Block (TCB) is a transport protocol knowledge structure (absolutely a suite of structures in lots of operations methods) that holds all the information a few connection. The memory footprint of a single TCB depends on what TCP options and different facets an implementation provides and has enabled for a connection. By and large, each TCB exceeds as a minimum 280 bytes, and in some running techniques presently takes greater than 1300 bytes. The TCP SYN-received state is used to indicate that the connection is most effective half open, and that the legitimacy of the request is still in question. The important aspect to notice is that the TCB is allocated based on reception of the SYN packets before the connection is wholly situated or the initiator's return reachability has been established.

This problem results in a transparent advantage DoS assault where incoming SYNs cause the allocation of so many TCBs that a bunch's kernel memory is exhausted. With the intention to prevent this memory exhaustion, running techniques usually accomplice a "backlog" parameter with a listening socket that sets a cap on the number of TCBs simultaneously within the SYN-received state. Even though this action protects a bunch's available

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

reminiscence useful resource from attack, the backlog itself represents yet another (smaller) resource liable to attack. And not using a room left within the backlog, it's inconceivable to provider new connection requests except some TCBs will also be reaped or otherwise eliminated from the SYN-got state. Depleting the backlog is the intention of the TCP SYN flooding assault, which makes an attempt to ship ample SYN segments to fill the whole backlog. The attacker makes use of supply IP addresses in the SYNs that are not more likely to set off any response that will free the TCBs from the SYN-bought state. Considering the fact that TCP makes an attempt to be risk-free, the goal host keeps its TCBs caught in SYN-received for a somewhat very long time earlier than giving up on the half connection and reaping them. Meanwhile, provider is denied to the appliance method on the listener for professional new TCP connection initiation requests. Determine 2 presents a simplification of the sequence of pursuits concerned in a TCP SYN flooding attack.

II. PACKET FILTERING TECHNIQUES

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports [20]. Network layer firewalls define packet filtering rule sets, which provide highly efficient security mechanisms. Packet filtering is also known as static filtering. When systems on a network communicate, they need to speak the same language, or protocol. One such protocol suite is TCP/IP, the primary communications language of the Internet. To facilitate such communications, the information you send needs to be broken down into manageable pieces called packets. Packet headers are small segments of information that are stuck at the beginning of a packet to identify it.

The IP portion of TCP/IP stands for Internet Protocol. It is responsible for identifying the packets (by their IP address) and for guiding them to their destination. IP packets are directed, or routed, by the values located in their packet headers. These identifiers hold information about where the packets came from (source address), where they are going (destination address), as well as other information describing the type of service the packet might support, among other things. When an IP packet arrives at a router, the router checks its destination to see whether it knows how to get to the place where the packet wants to go. If it does, it passes the packet to the appropriate network segment. The fact that a router passes any packet whose destination it is aware of is called implicit permit. Unless further security measures are added, all traffic is allowed in as well as out. For this reason, a method is required to control the information entering and exiting the interfaces of the router.

2.1 Common IP Filtering Techniques

i. Route filtering

Through this process, certain routes are not considered for inclusion in the local route database or not announced. Filters can be applied at the routers, before the routes are announced (output filtering) or as soon as a route is learned (input filtering). There are different reasons for filtering:

- To ensure that the use of private address space (RFC 1918) does not leak out into the global Internet, networks should block these prefixes in both their output and input filtering.
- When a site is multihued, announcing non-local routes to a neighbour different from the one it was learned from amounts to advertising the willingness to serve for transit. This is undesirable, unless suitable agreements are in place. You can avoid this issue by applying output filtering on these routes.
- An ISP will typically perform input filtering on routes learned from a customer to restrict them to the addresses actually assigned to that customer. Doing so makes address hijacking more difficult. Similarly, an ISP will perform input filtering on routes learned from other ISPs to protect its customers from address hijacking.

In some cases, routers have insufficient amounts of main memory to hold the full global BGP table. By applying input filtering on prefix length (eliminating all routes for prefixes longer than a given value), on AS count, or on some combination of the two, the local route database is limited to a subset of the global table. This practice is not recommended, as it can cause sub-optimal routing or even communication failures with small networks, and frustrate the traffic-engineering efforts of one’s peers.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

ii. Firewall filtering

A firewall is a device, a set of devices, or a software application designed to permit or deny network transmissions based upon a set of rules to protect networks from unauthorized access while permitting legitimate traffic to pass. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions. The different types of firewalls that can be defined depending on where the communication is taking place, where the communication is intercepted, and the state that is being traced.

- Network layer firewalls or packet filters operate at the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set defined by the administrator or applied by default. Modern firewalls can filter traffic based on many packet attributes such as source IP address, source port, destination IP address or port, or destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.
- Application layer firewalls work on the application level of the TCP/IP stack, intercepting all packets travelling to or from an application, dropping unwanted outside traffic from reaching protected machines, without acknowledgment to the sender. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.
- Mandatory access control (MAC) filtering or sandboxing protect vulnerable services by allowing or denying access based on the MAC address of specific devices allowed to connect to a specific network.
- Proxy servers or services can run on dedicated hardware devices or as software on a general-purpose machine, responding to input packets such as connection requests, while blocking other packets. Abuse of an internal system would not necessarily cause a security breach, although methods such as IP spoofing could transmit packets to a target network.

- Network address translation (NAT) functionality allows hiding the IP addresses of protected devices by numbering them with addresses in the “private address range”, as defined in RFC 1918. This functionality offers a defence against network reconnaissance

- Firewall filtering requires constant adjustments to reflect the latest security policies, threat conditions, and address holdings. Outdated policies such as blocking IPv6 by default, or blocking certain IP addresses that sends malicious traffic, or blocking a whole network/ISP/Country may need to be reviewed from time to time to ensure overall network visibility do not degrade as more and more traffic gets accidentally discarded.

iii. Email filtering

Email filtering is the manual or automatic processing of incoming emails to organize them according to set criteria (topic, sender, etc) and removal of spam and computer viruses. The filters allow clean messages to be delivered to the user’s mailbox, while redirecting tainted messages for delivery to a quarantine application for the user’s review, or even ignore them. Some mail filters are able to edit messages during processing, for example deactivating URLs in email messages to remove the threat before users click. Although less common, some companies inspect outgoing email to oversee that their employees comply with law requirements. Email filters operate through a variety of techniques from matching a regular expression, a keyword, or the sender email address. More advanced solutions use statistical document classification techniques, IP reputation, and complex image analysis algorithms to prevent messages from reaching protected mailboxes.

Email filtering becomes problematic when a blacklisted IP address is transferred to a new network. The new network may have the mail traffic from the blacklisted IP address blocked and will have to contact various blacklist maintainers to delist the address. APNIC will be able to provide assistance by confirming to the blocking parties that the blacklisted address has changed hands, as long as the transfer was properly registered in the APNIC Who is Database.

iv. Proxy Filter (Server)

Proxy filters, also known as application proxy servers, extend beyond the reach of packet filters by examining information from layers 4–7. A proxy server sits between the client and the destination working as a middleman between the two communicating parties. It requires the client to establish a session with the proxy itself, which in turn

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

creates a second session between itself and the destination. Consider, for instance, a client computer that requests information from a remote Web site. The client creates a session with the proxy server, which can then authenticate the user for valid access to the Internet before creating a second session between the Web site and itself. As the information comes back from the Web site, the proxy server examines layers 4–7 for a valid connection to the inside network.

v. Stateful Packet Filter—Stateful Inspection

This type of firewall combines the speed of packet filters with the enhanced security of stored session information typified by proxies. While traffic is being forwarded through the firewall, stateful inspections of the packets create slots in session flow tables. These tables contain source and destination IP addresses, port numbers, and TCP protocol information. Before traffic can travel back through the firewall, stateful inspections of the packets are cross-referenced to the session flow tables for an existing connection slot. If a match is found in the tables, the packets are forwarded; otherwise, the packets are dropped or rejected. The Cisco PIX firewall uses stateful inspection as its primary method to control traffic flow.

III. SUPPORT VECTOR MACHINE

A Support Vector Machine (SVM) [2] is a discriminative classifier formally defined by a separating hyper plane. In other words, given labeled training data (supervised learning), the algorithm outputs an optimal hyper plane which categorizes new examples. In two dimensional spaces this hyper plane is a line dividing a plane in two parts where in each class lay in either side [19].

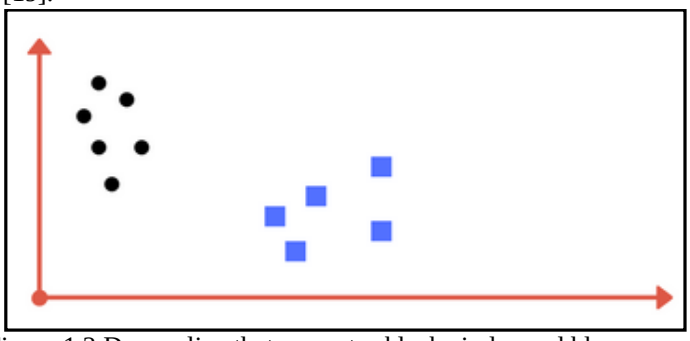


Figure 1.2 Draw a line that separates black circles and blue squares

You might have come up with something similar to following image. It fairly separates the two classes. Any point that is left of line falls into black circle class and on right falls into blue square class. Separation of classes. That's what SVM does. It finds out a line/ hyper-plane (in multidimensional space that separate outs classes).

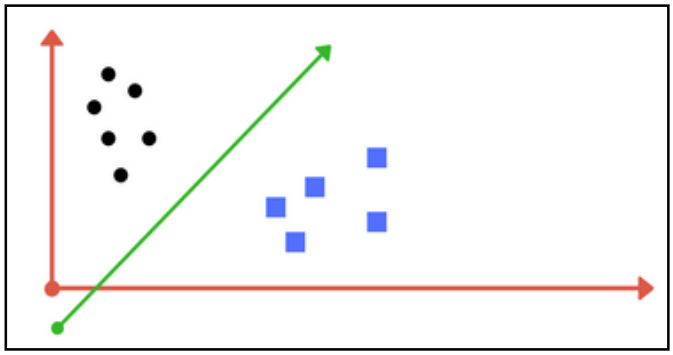


Figure 1.3 Sample cut to divide into two classes

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

3.1 Support vector machine classifiers

The key concept of SVMs, which were originally first developed for binary classification problems, is the use of hyper planes to define decision boundaries separating between data points of different classes [19].SVMs are able to handle both simple, linear, classification tasks, as well as more complex, i.e. nonlinear, classification problems. Both separable and no separable problems are handled by SVMs in the linear and nonlinear case. The idea behind SVMs is to map the original data points from the input space to a high- dimensional, or even infinite-dimensional, feature space such that the classification problem becomes simpler in the feature space.

3.2 Least squares support vector machine classifiers

It has been proposed to modify the SVM methodology by introducing a least squares loss function and equality instead of inequality constraints. Instead of solving a quadratic programming problem, the solution is obtained from a set of linear equations, significantly reducing the complexity and computational effort [19].

IV. PROPOSED ARCHITECTURE

In this section we present our proposed system, which can detects and prevent DDoS attack. In this proposed approach, DDoS defence systems are deployed in the network to detect and prevent DDoS attacks independently. We implemented this architecture by using Ossec, Wireshark log analysis tools and Support Vector Machine. Working process of the proposed architecture is described in next section.

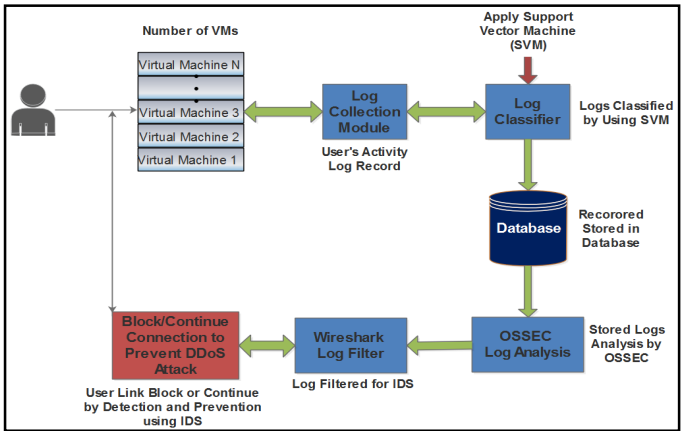


Fig 1.4 Proposed Architecture

4.1 WORKING STEPS OF PROPOSED METHODOLOGY

1. Number of user's connections is served by virtual machines.
2. User's activity logs are collected in Log Collection Module.
3. Log Classifier is used to classify and separates the user's logs according to performed activities. To classify these logs, we use support vector machine (SVM).
4. These classified logs are stored in database system.
5. Stored logs are analyzed by using OSSEC log analyzer tool.
6. Further these logs are tracks for diverse activities by Wireshark packet tracer tool.
7. If any diverse activity is found for connected users, the attack detection system detects it as a attack otherwise user's connection will remains continue.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

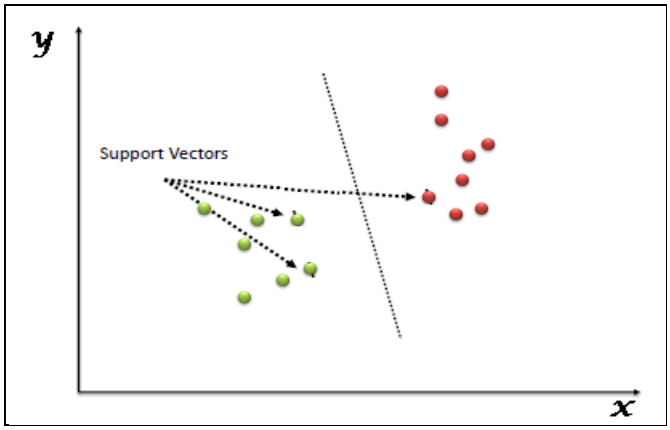
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

VI. RESULTS

"Support Vector Machine" (SVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiate the two classes very well (look at the below snapshot).



Support Vectors are simply the co-ordinates of individual observation. Support Vector Machine is a frontier which best segregates the two classes (hyper-plane/ line).

Tune Parameters of SVM

Tuning parameters value for machine learning algorithms effectively improves the model performance. Let's look at the list of parameters available with SVM.

I am going to discuss about some important parameters having higher impact on model performance, "kernel", "gamma" and "C".

kernel: We have already discussed about it. Here, we have various options available with kernel like, "linear", "rbf","poly" and others (default value is "rbf"). Here "rbf" and "poly" are useful for non-linear hyper-plane. Let's look at the example, where we've used linear kernel on two feature of iris data set to classify their class.

Have linear kernel

```
import numpy as np
import matplotlib.pyplot as plt
from sklearn import svm, datasets
# import some data to play with
idslog = datasets.load_idslog()
X = idslog.data[:, :2] # we only take the first two features. We could
 # avoid this ugly slicing by using a two-dim dataset
y = idslog.target
# we create an instance of SVM and fit out data. We do not scale our
# data since we want to plot the support vectors
C = 1.0 # SVM regularization parameter
svc = svm.SVC(kernel='linear', C=1,gamma=0).fit(X, y)
# create a mesh to plot in
x_min, x_max = X[:, 0].min() - 1, X[:, 0].max() + 1
y_min, y_max = X[:, 1].min() - 1, X[:, 1].max() + 1
```

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

```
h = (x_max / x_min)/100
xx, yy = np.meshgrid(np.arange(x_min, x_max, h),
 np.arange(y_min, y_max, h))
plt.subplot(1, 1, 1)
Z = svc.predict(np.c_[xx.ravel(), yy.ravel()])
Z = Z.reshape(xx.shape)
plt.contourf(xx, yy, Z, cmap=plt.cm.Paired, alpha=0.8)
plt.scatter(X[:, 0], X[:, 1], c=y, cmap=plt.cm.Paired)
plt.xlabel('Sepal length')
plt.ylabel('Sepal width')
plt.xlim(xx.min(), xx.max())
plt.title('SVC with linear kernel')
plt.show()
```

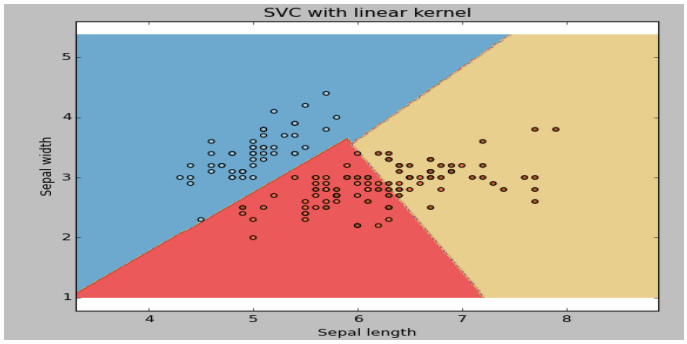


Figure 1.5 SVC with linear kernel

Change the kernel type to rbf in below line and look at the impact.

```
svc = svm.SVC(kernel='rbf', C=1,gamma=0).fit(X, y)
```

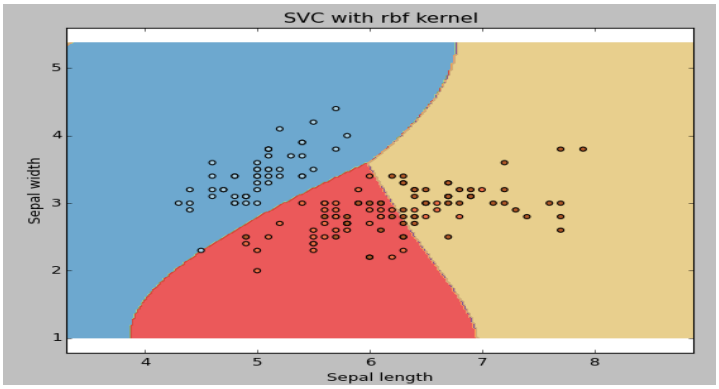


Figure 1.6 SVC with rbf kernel

gamma: Kernel coefficient for 'rbf', 'poly' and 'sigmoid'. Higher the value of gamma, will try to exact fit the as per training data set i.e. generalization error and cause over-fitting problem.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

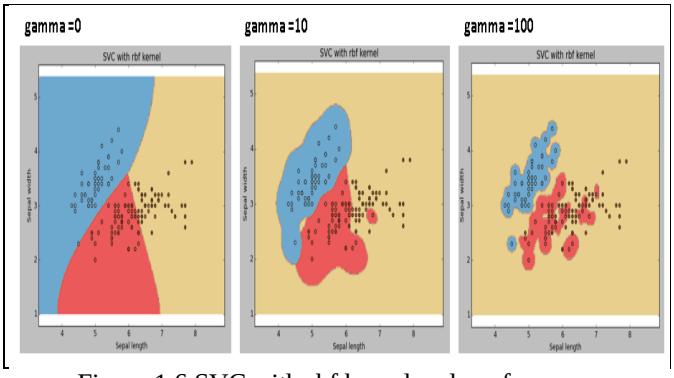


Figure 1.6 SVC with rbf kernel, value of gamma

C: Penalty parameter C of the error term. It also controls the tradeoff between smooth decision boundary and classifying the training points correctly.

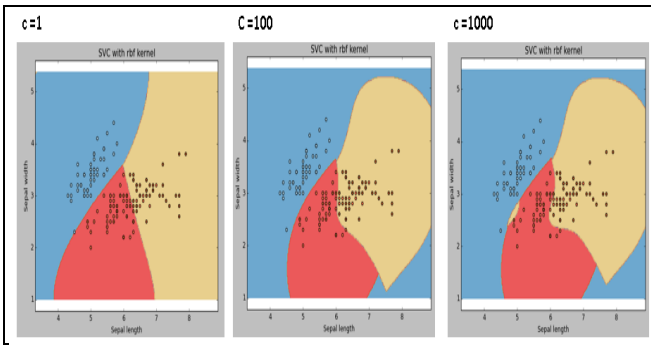


Figure 1.7 SVC with rbf kernel, value Penalty parameter C

Importing data

Once we have downloaded the data, the first thing we want to do is to load it in and inspect its structure. For this we will use pandas.

Pandas are a python library that gives us a common interface for data processing called a Data Frame. Data Frames are essentially excelling spreadsheets with rows and columns, but without the fancy UI excel offers. Instead, we do all the data manipulation programmatically. Pandas also have the added benefit of making it super simple to import data as it supports many different formats including excel spreadsheets, csv files, and even HTML documents.

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
plt.style.use('ggplot') # make plots look better
```

After having imported the libraries we are going to use, we can now read the datafile using pandas' read_csv() method.

```
df = pd.read_csv("logdata.csv")
```

Pandas automatically interpret the first line as column headers. If your dataset doesn't specify the column headers in first line, you can pass the argument header=None to the read_csv() function to interpret the whole document as data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Alternatively, you can also pass a list with the column names as the header parameter. To confirm that pandas has correctly read the csv file we can call df.head() to display the first five rows.

VII. COMPARISON OF EXISTING WORK AND PROPOSED WORK

Comparison between existing and proposed system is shown here:-

TABLE 1:-Classification performance measurements (**n=1000 and K=100**)

S. No	Parameters	Existing System		Proposed System	
		Accuracy	Sensitivity	Accuracy	Sensitivity
1	LS-SVM	99.5 %	95.3%	99.8%	96.4%
2	K-nearest	75%	93.5%	77.5%	94.8%
3	Multilayer Perceptron	88.3%	95.3%	90.2%	96.6%

Table 1.1 Comparison between existing and proposed system (n=1000 and K=100)

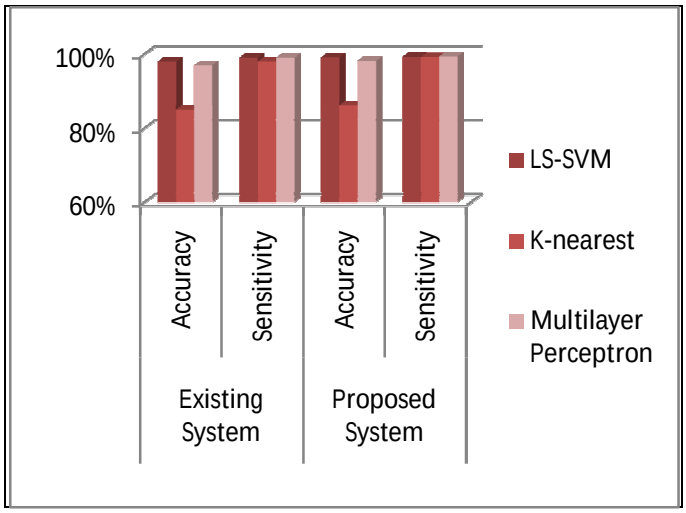


Figure 1.8 Comparison graph between existing and proposed system (n=1000 and K=100)

TABLE 2 :- Classification performance measurements (**n=2000 and K=200**)

S. No	Parameters	Existing System		Proposed System	
		Accuracy	Sensitivity	Accuracy	Sensitivity
1	LS-SVM	94.6 %	94%	95.9%	95.2%
2	K-nearest	80%	95%	82.1%	96.2%
3	Multilayer Perceptron	92%	97%	93.8%	98.3%

Table 1.2 Comparison between existing and proposed system (n=2000 and K=200)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

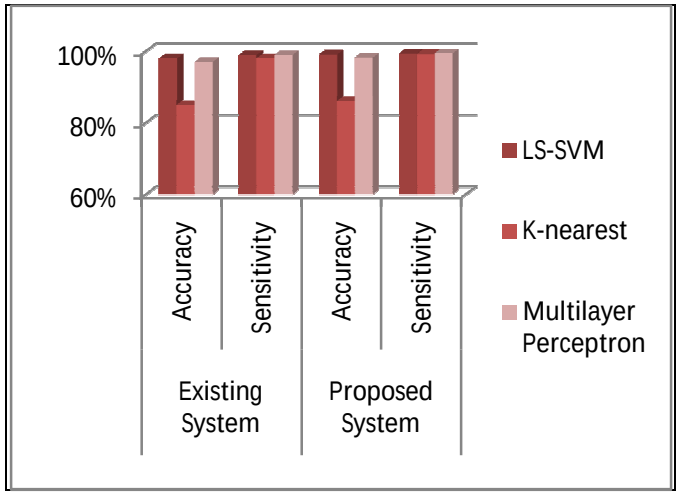


Figure 1.9 Comparison graph between existing and proposed system (n=2000 and K=200)

TABLE 3 :- Classification performance measurements **(n=5000 and K=300)**

S. No	Parameters	Existing System		Proposed System	
		Accuracy	Sensitivity	Accuracy	Sensitivity
1	LS-SVM	96%	98%	97.1%	99.2%
2	K-nearest	82%	96%	83.3%	97.1%
3	Multilayer Perceptron	95%	99%	96.5%	99.3%

Table 1.3 Comparison between existing and proposed system (n=5000 and K=300)

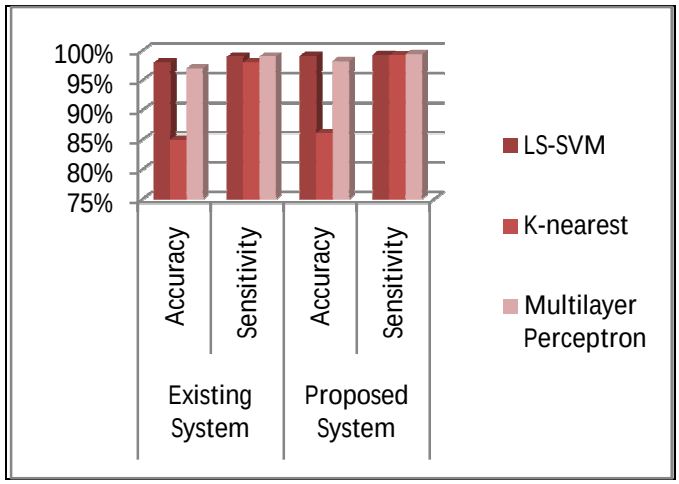


Figure 1.10 Comparison graph between existing and proposed system (n=5000 and K=300)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

TABLE 4 :- Classification performance measurements (**n=6000 and K=400**)

S. No	Parameters	Existing System		Proposed System	
		Accuracy	Sensitivity	Accuracy	Sensitivity
1	LS-SVM	98%	99%	99.1%	99.3%
2	K-nearest	85%	98%	86.1%	99.2%
3	Multilayer Perceptron	97%	99%	98.2%	99.4%

Table 1.4 Comparison between existing and proposed system (n=6000 and K=400)

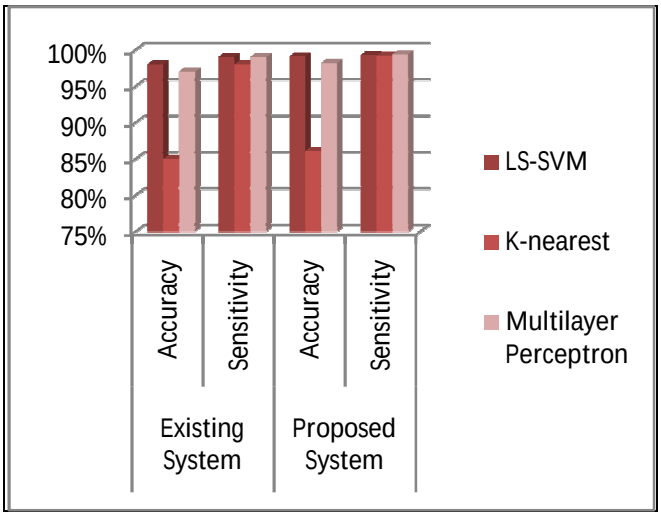


Figure 1.11 Comparison graph between existing and proposed system (n=6000 and K=400)

VIII. CONCLUSION

Security issues related to the cloud computing are relevant to various stakeholders for an informed cloud adoption decision. Apart from data breaches, the cyber security research community is revisiting the attack space for cloud-specific solutions as these issues affect budget, resource management, and service quality. Distributed Denial of Service (DDoS) attack is one such serious Attack in the cloud space. In this research, we present developments related to DDoS attack mitigation solutions in the cloud. In this research, we analyze the impact of cloud computing and DDoS attack defence. Based on our analysis, we identify the challenges and the benefits raised by these new technologies. We claim that with careful design could help with DDoS attack protection. To substantiate our finding, we proposed our solution of defending DDoS attack architecture. We also carried out a simulation study using real network traces to evaluate the performance. The results show that our proposed model is successful in dealing with the new challenges raised. The detection algorithm is fast enough to perform online packet inference and it achieves a high detection rate. The proposed model update process saves a significant amount of time compared to regenerating a model while suffering hardly any performance loss in terms of detection accuracy.

In the future, we aim to extend system to completely overcome the problem of DDoS with more efficiency as well as to improve the proposed work to identify the attackers even when they satisfy the known parameter value.

REFERENCES

1. Saman Taghavi Zargar, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communications Surveys & Tutorials, published online Feb. 2013.
2. Jan Luts, Fabian Ojeda, "A tutorial on support vector machine-based methods for classification problems in chemometrics", Analytica Chimica Acta 665 (2010) 129–145, © 2010 Elsevier B.V. All rights reserved. doi:10.1016.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

3. Aqeel Sahi, David Lai, Yan Li, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment", date of publication April 6, 2017, date of current version May 17, 2017. Digital Object Identifier 10.1109/ACCESS.2017.2688460, 2017 IEEE.
4. Qiao Yan and F. Richard Yu, "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing", Security And Privacy In Emerging Networks, 0163-6804/15/$25.00 © 2015 IEEE.
5. Rashmi V. Deshmukh, Kailas K. Devadkar, "Understanding DDoS Attack & Its Effect In Cloud Environment", Procedia Computer Science 49 (2015) 202 – 210, 2015 Published by Elsevier.
6. K.Santhi Sri1, PRSM Lakshmi, "DDoS Attacks, Detection Parameters and Mitigation in Cloud Environment", Proceedings of National Conference on Recent Advances in Computer Science & Engineering (NCRACSE-2017), Volume 3 | Special Issue 01 | February 2017.
7. Khalid A. Fakeeh, "An Overview of DDOS Attacks Detection and Prevention in the Cloud", International Journal of Applied Information Systems (IJAIS), Volume 11 – No. 7, December 2016.
8. Rabia Latif , Haider Abbas, Saïd Assar, "Distributed Denial of Service (DDoS) Attack in Cloud- Assisted Wireless Body Area Networks: A Systematic Literature Review", Published online: 14 September 2014# Springer.
9. Anteneh Girma, Moses Garuba," Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment", 2015 12th International Conference on Information Technology - New Generations, 978-1-4799-8828-0/15 $31.00 © 2015 IEEE.
10. Opeyemi.A. Osanaiye, "Short Paper: IP Spoofing Detection for Preventing DDoS Attack in Cloud Computing", 2015 18th International Conference on Intelligence in Next Generation Networks ©2015 IEEE.
11. Kanchan ,Harwant Singh Arri, "A Review Paper on Preventing DDOS Attack and Black Hole Attack with MANETs Protocols", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 5 may, 2014.
12. Baldev Singh, Rajiv Mahajan, "Detecting DDOS Attacks in Cloud- A Novel Approach", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 5, May 2016.
13. Baldev Singh, Dr. S. N. Panda, "Defending Against DDOS Flooding Attacks- A Data Streaming
Approach", © 2015, IJCIT All Rights Reserved.
14. Baldev Singh, S.N. Panda, "An Adaptive Approach to Mitigate Ddos Attacks in Cloud", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 10, 2015.
15. Gaurav Somani, Manoj Singh Gaur, "DDoS Attacks in Cloud Computing:Issues, Taxonomy, and Future Directions", Computer Communications, Volume 107, 2017, Preprint @ Elsevier.
16. Wei Wei ; Feng Chen ; Yingjie Xia ; Guang Jin, "A Rank Correlation Based Detection against Distributed Reflection DoS Attacks", IEEE Communications Letters , Volume: 17, Issue: 1, January 2013 .
17. Bing Wang, Yao Zheng, Wenjing Lou, Y. Thomas Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking", Computer Networks 81 (2015) 308–319 @ 2015 Elsevier.
18. Angelos D. Keromytis, "SOS: An Architecture For Mitigating DDoS Attacks", Journal On Selected Areas In Communications, VOL. 21, c 2003 IEEE.
19. DalimaParwani, AmitDutta, "Various Techniques of DDoS Attacks Detection and Prevention at Cloud: A Survey", Orient. J. Comp. Sci. & Technol., Vol. 8(2), 110-120 (2015).
20. Opeyemi.A. Osanaiye, Mqhele Dlodlo, "TCP/IP Header Classification for Detecting Spoofed
DDoS Attack in Cloud Environment", ©2015 IEEE.
21. Khaled Salah, Khalid Elbadawi, "Performance Modeling and Analysis of Network Firewalls", IEEE Transactions On Network And Service Management, Vol. 9, No. 1, March 2012.
22. Wanchun Dou, Qi Chen, Jinjun Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment", Future Generation Computer Systems 29 (2013) © 2012 Elsevier.