Detection and Reduction of DDOS Attack Using IDS Tools

S.Emearld Jenifer Mary [1], C.Nalini [2]
[1,2]Bharath Institute of Higher Education and Research, Chennai.

Abstract

In recent scenario, the Cloud provides ultimate solutions for the new age of computing with some features like multi tenancy and agility. The major concern is the data available with the customers while the attackers attained all the important data wherever the cloud area is compromised. The vital problem in the cloud computing is one and only security issues. The key idea of our proposed system is that IDS, it could be used to protect the various protocol change. All the routers have faced the same security issues so that all other protocols are need to be coordinate with each other. Hence we designed the perfect system called IDS to become safety from the attacks. The Intrusion Detection System is a basic key idea to monitor the attackers going to attack and how to protect routers from the various attacks. So, here we proposed IDS with signature controls attackd with the same time monitored the packet movements.

Keywords— *Dsitributed Denial of service, Intrucion detection System, Interconnected Network.*

I.INTRODUCTION

Network is the sources of interconnection systems which could transfer the data between numerous numbers of computer. The important files can be hacked while the data transfer from one end to another end. The security is the only challenges we have faced through data transfer. So that we have created very strict regulations for data transferring in the internet.

Challenges of Network Issues

Misleading of the information can be prevented by using some safety measures like

i) Action taken on confidential violation
ii) Data damage
iii) Computation of data

We are creating an IDS which tends give some safety regarding the starvation from bandwidth attack. This means that the packet signature is already inside IDS protect against this kind of attack. From the findings , the packets of an IDS router can take impropriate steps to prevent the attack from happening.

The attacker communicates with the army of zombies which are called botnet and make those PCs send packets into network towards the target server. To protect this attack there are many algorithms but the main problem is that these algorithms need to be not in to two three but all the other routers to. But as we know that it is not possible that all routers have same algorithm as we are using for the router we tries to protect [3]. Because of this problem to protect router we need one protection mechanism such that it can protect router without relying on any other router.

Modules of IDS

Data gathering: The radio transmission range are combined the network in very normal position. [1].

Profile-generation: this module consists of two components

1. Data preparation: here the collected data are prepared for creating normal behavior profile. Processes like filtering, aggregation, data suppression are applied here.
2. Profiler (Profile generator): the second phase is made up of several techniques like clustering, classification rule mining or SVM where normal profile is made by the pre-processed data [5].

Anomaly Detection: This phase detect anomaly in the network with the help of derived rule set the data test profiles when combined with already expected profiles.. Suppose some rule generated from test data was not previously available in normal profile then it will be detected as anomaly.

Decision tacking system: when any anomaly rule trigger that will be attended locally as well as globally by giving alert to the neighbours when the support and confidence of anomaly rule goes above tolerated level. Here are some attack those are possible at different layer.

II. CLOUD- DDOS ATTACK

The major cloud providers are concentrated on the hackers attack like DDoS attack and also observe the cloud users feedback. The flood and cloud attack can be viewed very seriously shown in fig 1. make over the indirect or direct attack [6].

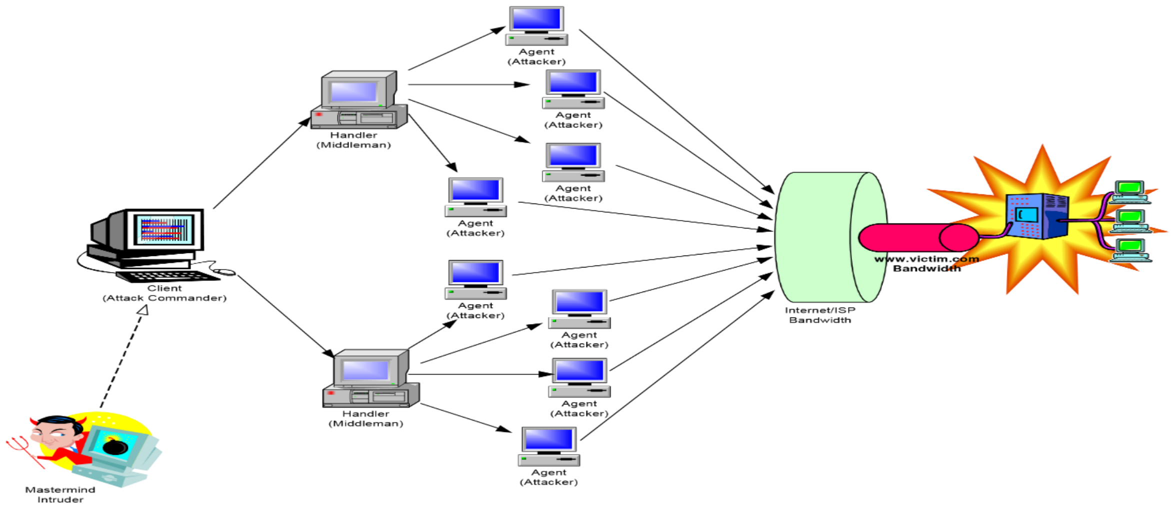


Figure 1: A typical DDoS Attack

III. Components of IDS

The large array of IDS availability gives certain security issues and correction. Since, we have lots of most common components are given in the list.

SNORT – The SNORT is the very important components which used to protect from the vulnerability using signature.

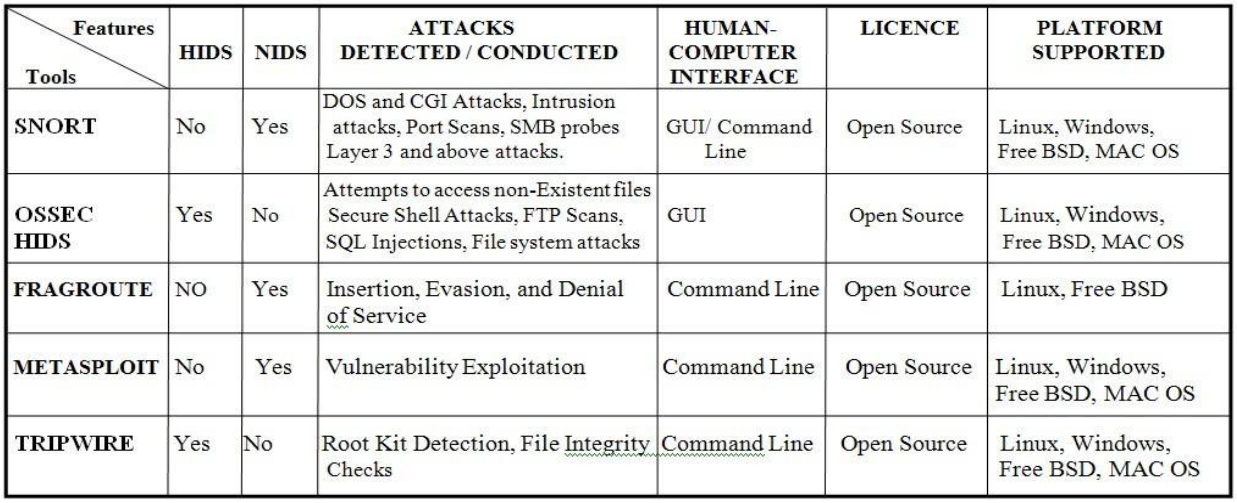
OSSEC – The Host based Intrusion detection system (HIDS) provides real time alerting and immediate response from cloud hackers.

FRAGROUTE –The most important router is the fragmenting router because it shows launch of attackers and also prevent the IP based attacks.

METASPLOIT – the least corners of internet used to prevent shell code.

TRIPWIRE –the change occurs in improper way could be identified by TRIPWIRE.

Table 1: Comparison of IDS Tools



Features / Tools	HIDS	NIDS	ATTACKS DETECTED / CONDUCTED	HUMAN-COMPUTER INTERFACE	LICENCE	PLATFORM SUPPORTED
SNORT	No	Yes	DOS and CGI Attacks, Intrusion attacks, Port Scans, SMB probes Layer 3 and above attacks.	GUI/ Command Line	Open Source	Linux, Windows, Free BSD, MAC OS
OSSEC HIDS	Yes	No	Attempts to access non-Existent files Secure Shell Attacks, FTP Scans, SQL Injections, File system attacks	GUI	Open Source	Linux, Windows, Free BSD, MAC OS
FRAGROUTE	NO	Yes	Insertion, Evasion, and Denial of Service	Command Line	Open Source	Linux, Free BSD
METASPLOIT	No	Yes	Vulnerability Exploitation	Command Line	Open Source	Linux, Windows, Free BSD, MAC OS
TRIPWIRE	Yes	No	Root Kit Detection, File Integrity Checks	Command Line	Open Source	Linux, Windows, Free BSD, MAC OS

IV. OVERVIEW OF INTRUSION DETECTION SYSTEM (IDS)

In network security, we have proposed various tools such as antivirus, firewall etc. Therefore one of the solutions is using an IDS , the system also detects hackers attacks and threats of various intruders due to the policy which applied to Firewall inbound and outbound[1-4].

The most vital two sub system of IDS are given as:

- **Network Intrusion Detection System (NIDS):** The NIDS is the important challenges in the cloud based hackers [15]. Fig. 5 shows a NIDS and HIDS.
- **Host Intrusion Detection System (HIDS):** It could not support to monitored the all network but also gives preventive measures from individual systems.

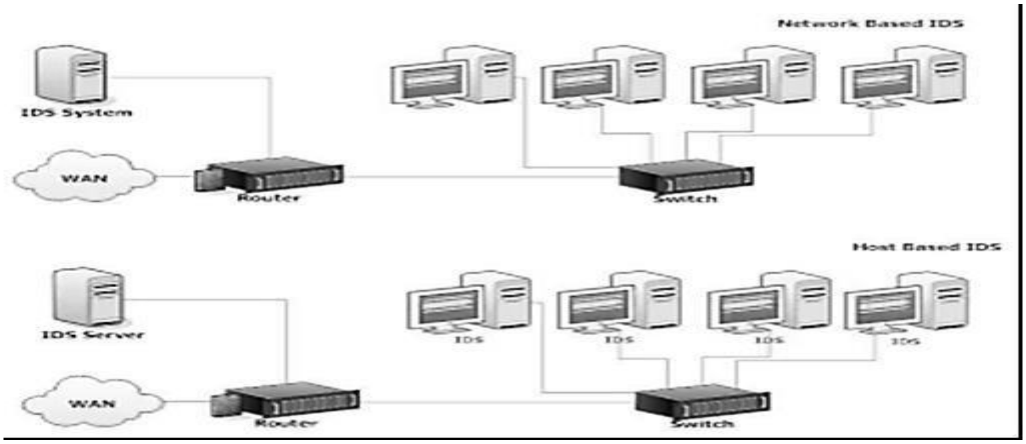
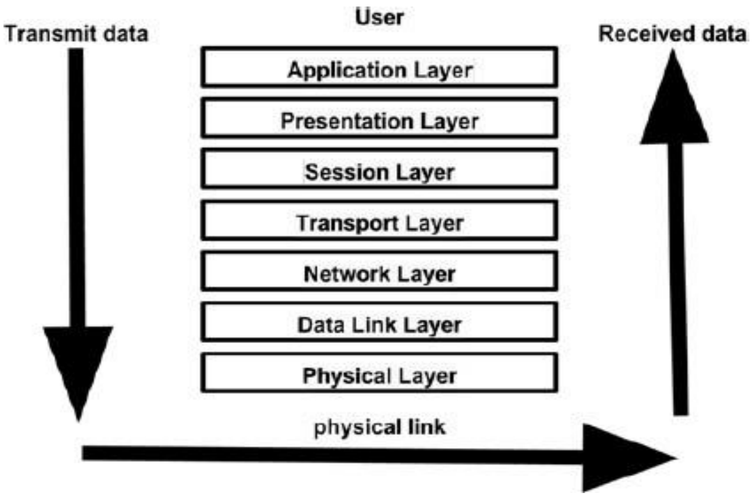


Figure 2: HIDS & NIDS Structure

Copyright ⓒ2020 SERSC

The below diagram shows the OSI layers with that we are testing network and application layers.

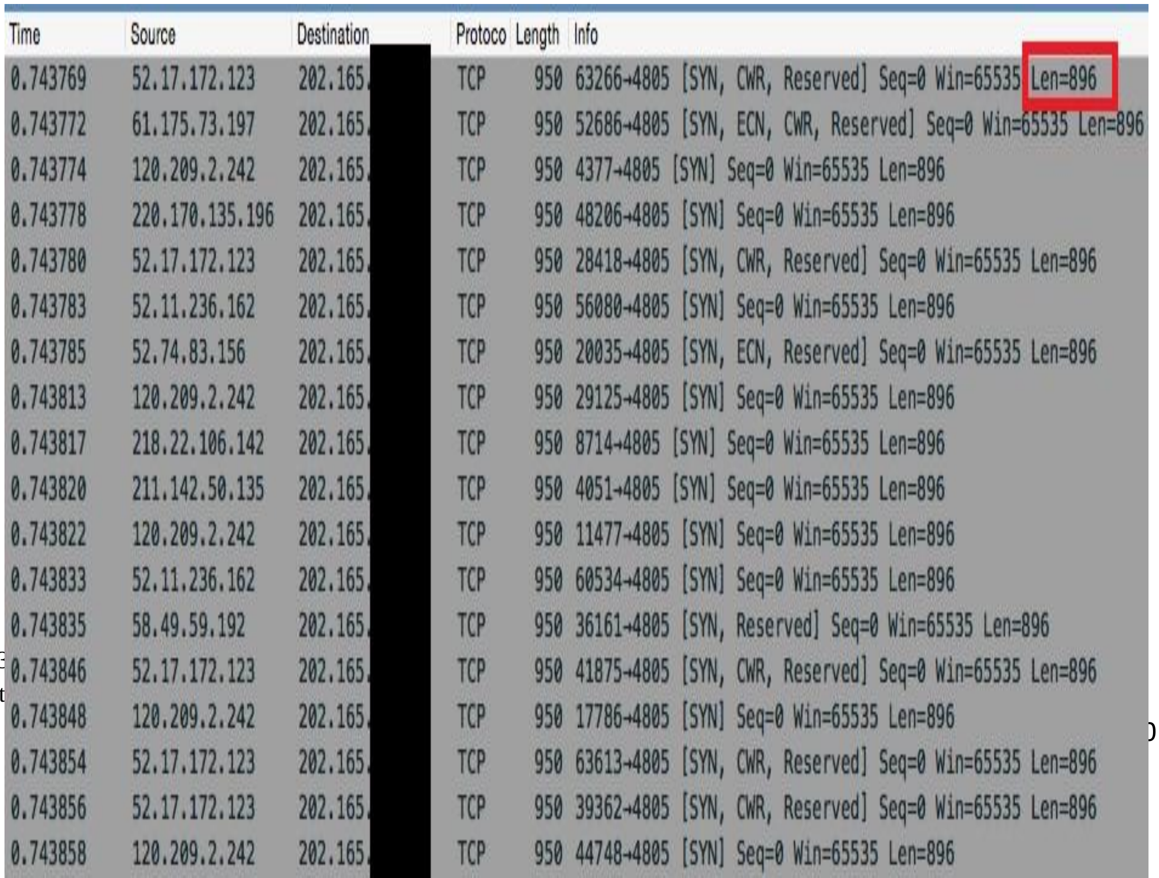
Figure 3: OSI Seven Layers



Inside Look at a DDoS Attack

The image below shows network traffic captured during the DDoS attack. Unfortunately, it is easy for an attacker to create SYN packets and use them to launch a volumetric DDoS attack. This attack can saturate the Internet connection of your organization even before hitting any state full network device like the Firewall and Load Balancer. Notice the SYN packets with the Len=896 bytes payload highlighted in red. As one can see, the attacker was sending a high rate of SYN packets.

Table 2:List of the top attackers' IP addresses

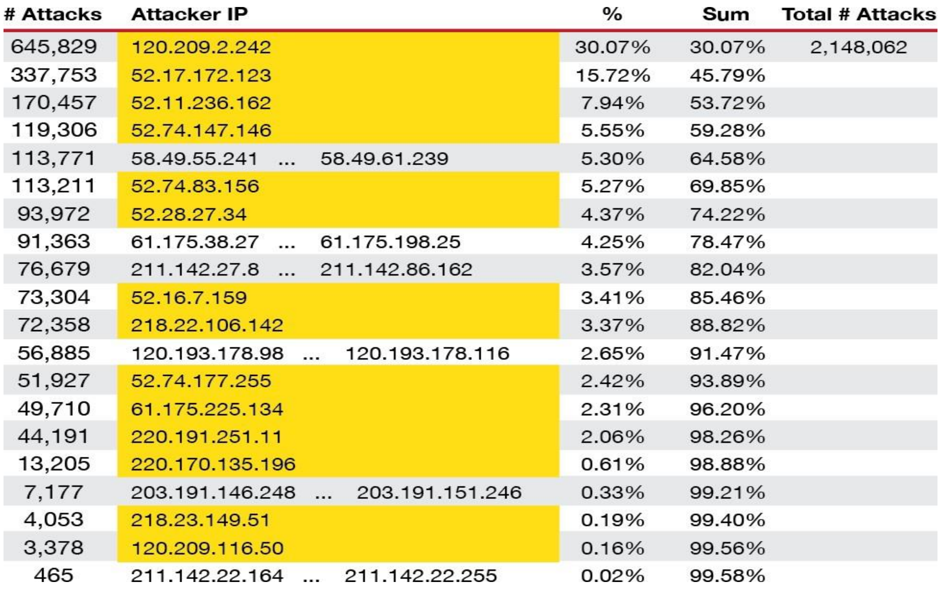


Time	Source	Destination	Protoco	Length	Info
0.743769	52.17.172.123	202.165.[redacted]	TCP	950	63266→4805 [SYN, CWR, Reserved] Seq=0 Win=65535 Len=896
0.743772	61.175.73.197	202.165.[redacted]	TCP	950	52686→4805 [SYN, ECN, CWR, Reserved] Seq=0 Win=65535 Len=896
0.743774	120.209.2.242	202.165.[redacted]	TCP	950	4377→4805 [SYN] Seq=0 Win=65535 Len=896
0.743778	220.170.135.196	202.165.[redacted]	TCP	950	48206→4805 [SYN] Seq=0 Win=65535 Len=896
0.743780	52.17.172.123	202.165.[redacted]	TCP	950	28418→4805 [SYN, CWR, Reserved] Seq=0 Win=65535 Len=896
0.743783	52.11.236.162	202.165.[redacted]	TCP	950	56080→4805 [SYN] Seq=0 Win=65535 Len=896
0.743785	52.74.83.156	202.165.[redacted]	TCP	950	20035→4805 [SYN, ECN, Reserved] Seq=0 Win=65535 Len=896
0.743813	120.209.2.242	202.165.[redacted]	TCP	950	29125→4805 [SYN] Seq=0 Win=65535 Len=896
0.743817	218.22.106.142	202.165.[redacted]	TCP	950	8714→4805 [SYN] Seq=0 Win=65535 Len=896
0.743820	211.142.50.135	202.165.[redacted]	TCP	950	4051→4805 [SYN] Seq=0 Win=65535 Len=896
0.743822	120.209.2.242	202.165.[redacted]	TCP	950	11477→4805 [SYN] Seq=0 Win=65535 Len=896
0.743833	52.11.236.162	202.165.[redacted]	TCP	950	60534→4805 [SYN] Seq=0 Win=65535 Len=896
0.743835	58.49.59.192	202.165.[redacted]	TCP	950	36161→4805 [SYN, Reserved] Seq=0 Win=65535 Len=896
0.743846	52.17.172.123	202.165.[redacted]	TCP	950	41875→4805 [SYN, CWR, Reserved] Seq=0 Win=65535 Len=896
0.743848	120.209.2.242	202.165.[redacted]	TCP	950	17786→4805 [SYN] Seq=0 Win=65535 Len=896
0.743854	52.17.172.123	202.165.[redacted]	TCP	950	63613→4805 [SYN, CWR, Reserved] Seq=0 Win=65535 Len=896
0.743856	52.17.172.123	202.165.[redacted]	TCP	950	39362→4805 [SYN, CWR, Reserved] Seq=0 Win=65535 Len=896
0.743858	120.209.2.242	202.165.[redacted]	TCP	950	44748→4805 [SYN] Seq=0 Win=65535 Len=896

Attackers' IP addresses and the number of SYN packets they've sent over a period of about 70 the table on the following page shows a list of the top seconds.

This investigation suggests that the spoofed traffic was generated by 10-15 compromised or rented servers that were all running on hosting providers which do not prevent their clients from sending spoofed IP traffic. This investigation suggests that the spoofed traffic was generated by 10-15 compromised or rented servers that were all running on hosting providers which do not prevent their clients from sending spoofed IP traffic. This investigation suggests that the spoofed traffic was generated by 10-15 compromised or rented servers that were all running on hosting providers which do not prevent their clients from sending spoofed IP traffic [5].

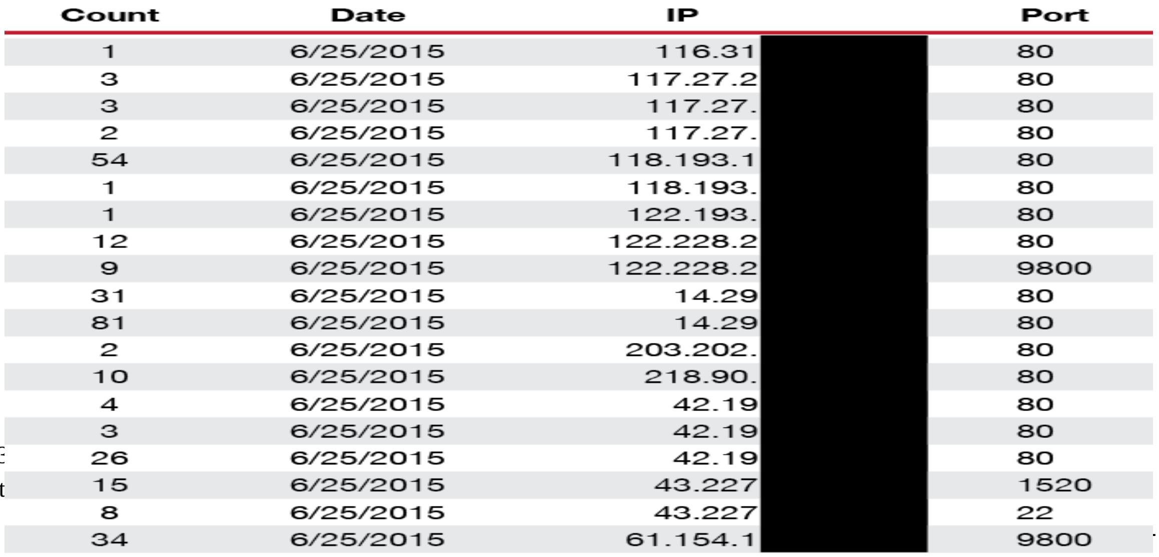
Table 3: IP traffic



# Attacks	Attacker IP	%	Sum	Total # Attacks
645,829	120.209.2.242	30.07%	30.07%	2,148,062
337,753	52.17.172.123	15.72%	45.79%	
170,457	52.11.236.162	7.94%	53.72%	
119,306	52.74.147.146	5.55%	59.28%	
113,771	58.49.55.241 ... 58.49.61.239	5.30%	64.58%	
113,211	52.74.83.156	5.27%	69.85%	
93,972	52.28.27.34	4.37%	74.22%	
91,363	61.175.38.27 ... 61.175.198.25	4.25%	78.47%	
76,679	211.142.27.8 ... 211.142.86.162	3.57%	82.04%	
73,304	52.16.7.159	3.41%	85.46%	
72,358	218.22.106.142	3.37%	88.82%	
56,885	120.193.178.98 ... 120.193.178.116	2.65%	91.47%	
51,927	52.74.177.255	2.42%	93.89%	
49,710	61.175.225.134	2.31%	96.20%	
44,191	220.191.251.11	2.06%	98.26%	
13,205	220.170.135.196	0.61%	98.88%	
7,177	203.191.146.248 ... 203.191.151.246	0.33%	99.21%	
4,053	218.23.149.51	0.19%	99.40%	
3,378	120.209.116.50	0.16%	99.56%	
465	211.142.22.164 ... 211.142.22.255	0.02%	99.58%	

Table 4: Every day different servers are attacked on different ports

V.PROPOSED WORK



Count	Date	IP	Port
1	6/25/2015	116.31 [redacted]	80
3	6/25/2015	117.27.2 [redacted]	80
3	6/25/2015	117.27. [redacted]	80
2	6/25/2015	117.27. [redacted]	80
54	6/25/2015	118.193.1 [redacted]	80
1	6/25/2015	118.193. [redacted]	80
1	6/25/2015	122.193. [redacted]	80
12	6/25/2015	122.228.2 [redacted]	80
9	6/25/2015	122.228.2 [redacted]	9800
31	6/25/2015	14.29 [redacted]	80
81	6/25/2015	14.29 [redacted]	80
2	6/25/2015	203.202. [redacted]	80
10	6/25/2015	218.90. [redacted]	80
4	6/25/2015	42.19 [redacted]	80
3	6/25/2015	42.19 [redacted]	80
26	6/25/2015	42.19 [redacted]	80
15	6/25/2015	43.227 [redacted]	1520
8	6/25/2015	43.227 [redacted]	22
34	6/25/2015	61.154.1 [redacted]	9800

The signature based cloud security system can be prosed to improve the system performance by means of Intrusion Detection System [10],[11.]. If the packet signature identified from the database , we are detecting the ICMP packets not another one,[1],[2].

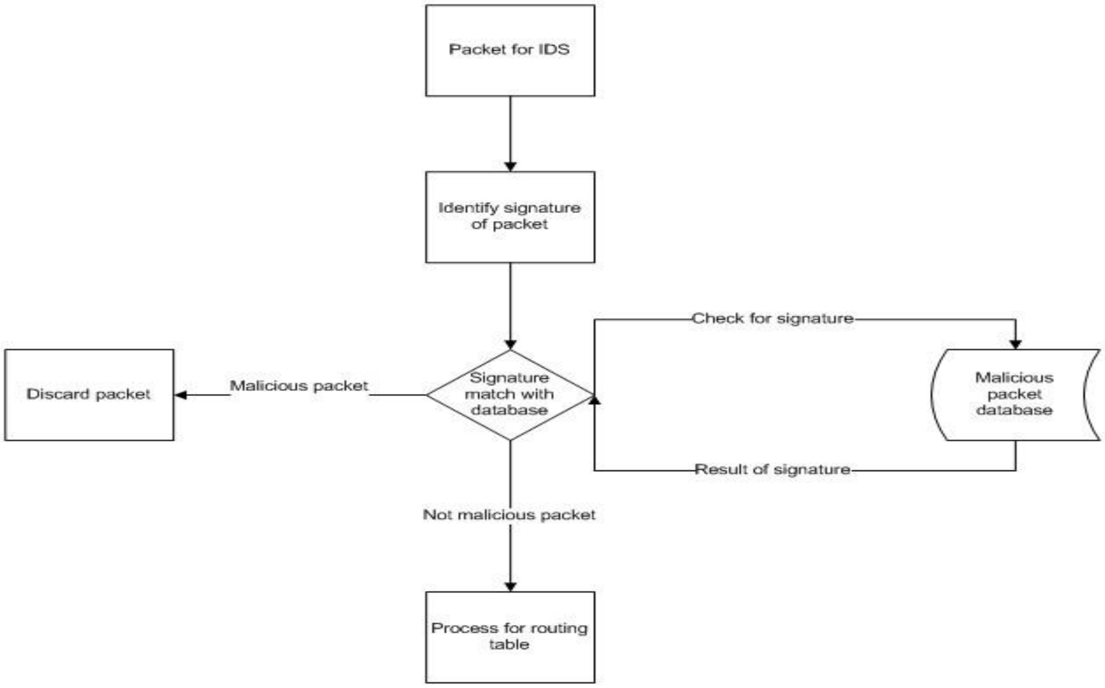

Packet for IDS
Identify signature of packet
Check for signature
Malicious packet database
Signature match with database
Malicious packet
Discard packet
Result of signature
Not malicious packet
Process for routing table

Figure 4: Simple IDS flowchart

The packet stay back within the network it creates DDoS attack and also with the help of signature based IS setup to gives more system favor. The ICMP, the size of the packets not more than 76 bytes identified from all the normal packets [12]. The payload are also the vita;l components have the sane signature with big size of 1300 and 1400 bytes to detects the TCP attack detection of signature needs to be checked [7].

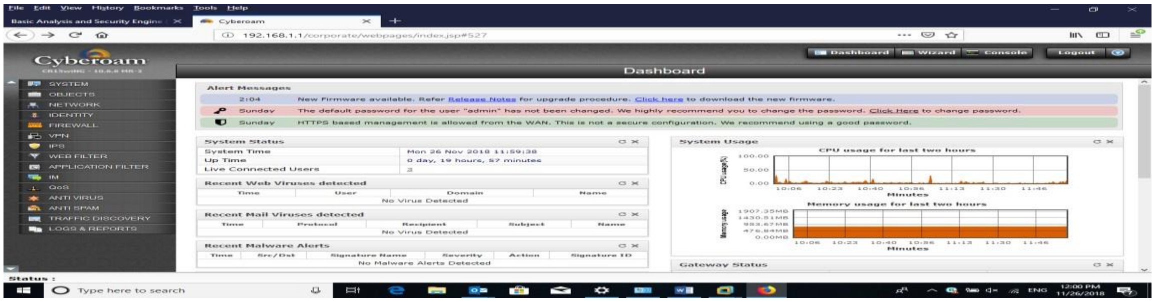
VI. RESULT AND DISCUSSION

Now days DDoS Attack is more sophisticated, the vulnerabilities shows the servers with patch and alarm rate users can be challenging. Exploit attacks can be devastating and are often undetectable prevent the Attack any how identify systematic methods for intrusion detection. Solution must be Signature based and Anomalies based together hybrid based solution [13To prevent intrusion in the network, make used firewall provide the end point[1].

Firewall rules (also called firewall policies) are a major challenge for network security administrators, making it important for companies and organizations, especially those distributed enterprise operations. To have and implement a firewall policy management solution.

First start with latest conventional firewall, beginning applied the IPS policy. Configured the inbound and outbound policy according to the customize requirements, it will be categorize to general policy, above rules prevent the unauthorized access to the system. WAN to LAN, DMZ to LAN [14].

Apply policy DMZ to WAN



Alert Messages

	2:04	New Firmware available. Refer Release Notes for upgrade procedure. Click here to download the new firmware.
	Sunday	The default password for the user "admin" has not been changed. We highly recommend you to change the password. Click Here to change password.
	Sunday	HTTPS based management is allowed from the WAN. This is not a secure configuration. We recommend using a good password.

System Status

System Time	Mon 26 Nov 2018 11:59:38
Up Time	0 day, 19 hours, 57 minutes
Live Connected Users	3

Recent Web Viruses detected

Time	User	Domain	Name
No Virus Detected			

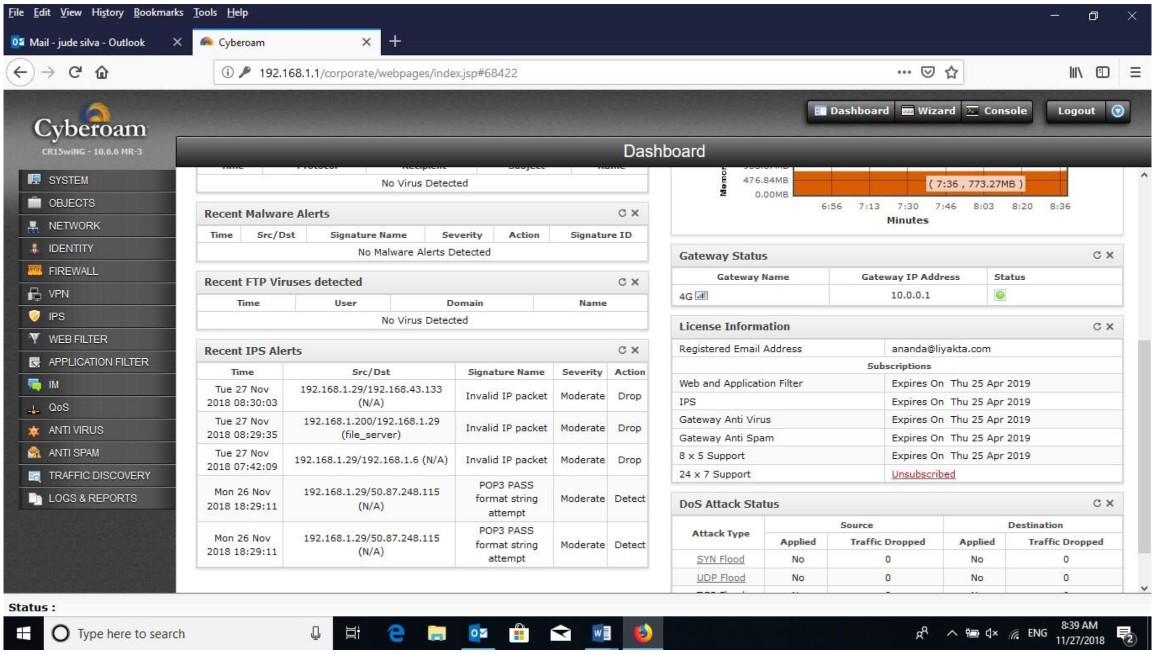
Recent Mail Viruses detected

Time	Protocol	Recipient	Subject	Name
No Virus Detected				

Recent Malware Alerts

Time	Src/Dst	Signature Name	Severity	Action	Signature ID
No Malware Alerts Detected					

Figure 5: Detected the viruses in the firewall.



No Virus Detected

Recent Malware Alerts

Time	Src/Dst	Signature Name	Severity	Action	Signature ID
No Malware Alerts Detected					

Recent FTP Viruses detected

Time	User	Domain	Name
No Virus Detected			

Recent IPS Alerts

Time	Src/Dst	Signature Name	Severity	Action
Tue 27 Nov 2018 08:30:03	192.168.1.29/192.168.43.133 (N/A)	Invalid IP packet	Moderate	Drop
Tue 27 Nov 2018 08:29:35	192.168.1.200/192.168.1.29 (file_server)	Invalid IP packet	Moderate	Drop
Tue 27 Nov 2018 07:42:09	192.168.1.29/192.168.1.6 (N/A)	Invalid IP packet	Moderate	Drop
Mon 26 Nov 2018 18:29:11	192.168.1.29/50.87.248.115 (N/A)	POP3 PASS format string attempt	Moderate	Detect
Mon 26 Nov 2018 18:29:11	192.168.1.29/50.87.248.115 (N/A)	POP3 PASS format string attempt	Moderate	Detect

Gateway Status

Gateway Name	Gateway IP Address	Status
4G	10.0.0.1	🟩

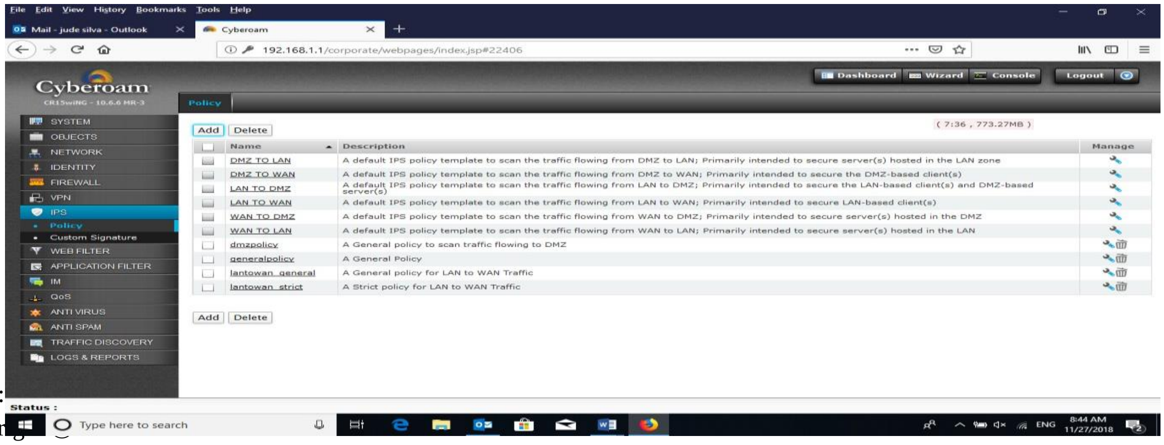
License Information

Registered Email Address	ananda@liyakta.com
Subscriptions	
Web and Application Filter	Expires On Thu 25 Apr 2019
IPS	Expires On Thu 25 Apr 2019
Gateway Anti Virus	Expires On Thu 25 Apr 2019
Gateway Anti Spam	Expires On Thu 25 Apr 2019
8 x 5 Support	Expires On Thu 25 Apr 2019
24 x 7 Support	Unsubscribed

DoS Attack Status

Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
SYN Flood	No	0	No	0
UDP Flood	No	0	No	0

Figure 6: Forming the IPS Alerts

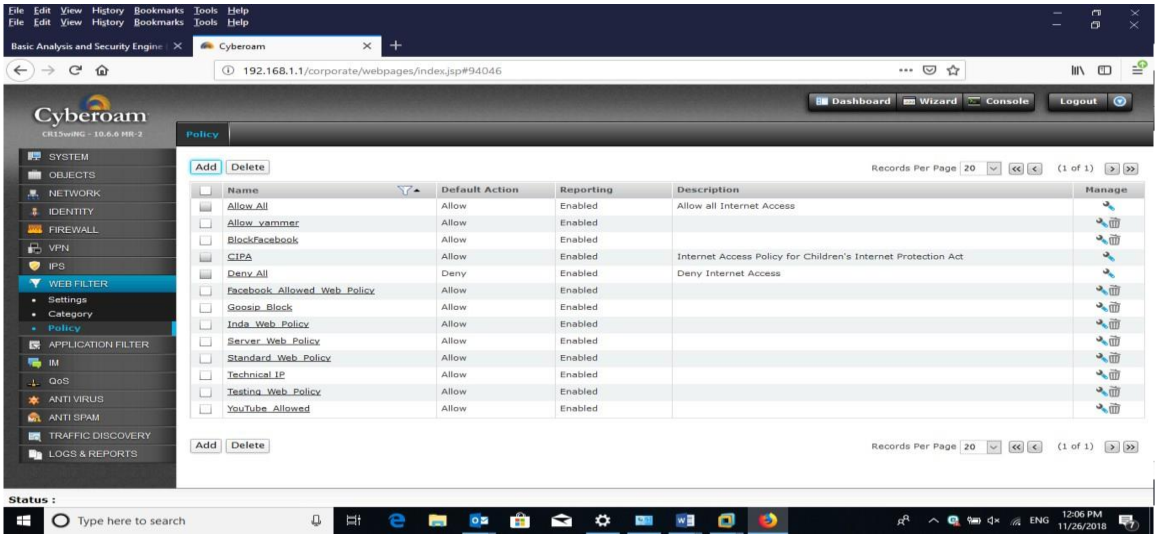


□	Name	Description	Manage
□	DMZ TO LAN	A default IPS policy template to scan the traffic flowing from DMZ to LAN; Primarily intended to secure server(s) hosted in the LAN zone	
□	DMZ TO WAN	A default IPS policy template to scan the traffic flowing from DMZ to WAN; Primarily intended to secure the DMZ-based client(s)	
□	LAN TO DMZ	A default IPS policy template to scan the traffic flowing from LAN to DMZ; Primarily intended to secure the LAN-based client(s) and DMZ-based server(s)	
□	LAN TO WAN	A default IPS policy template to scan the traffic flowing from LAN to WAN; Primarily intended to secure LAN-based client(s)	
□	WAN TO DMZ	A default IPS policy template to scan the traffic flowing from WAN to DMZ; Primarily intended to secure server(s) hosted in the DMZ	
□	WAN TO LAN	A default IPS policy template to scan the traffic flowing from WAN to LAN; Primarily intended to secure server(s) hosted in the LAN	
□	dmzpolicy	A General policy to scan traffic flowing to DMZ	
□	generalpolicy	A General Policy	
□	lantowan_general	A General policy for LAN to WAN Traffic	
□	lantowan_strict	A Strict policy for LAN to WAN Traffic	

Figure 7: IP policy to scan the traffic flowing

Spores if apply the rules DMZ to LAN, a default IP policy to scan the traffic flowing from DMZ.

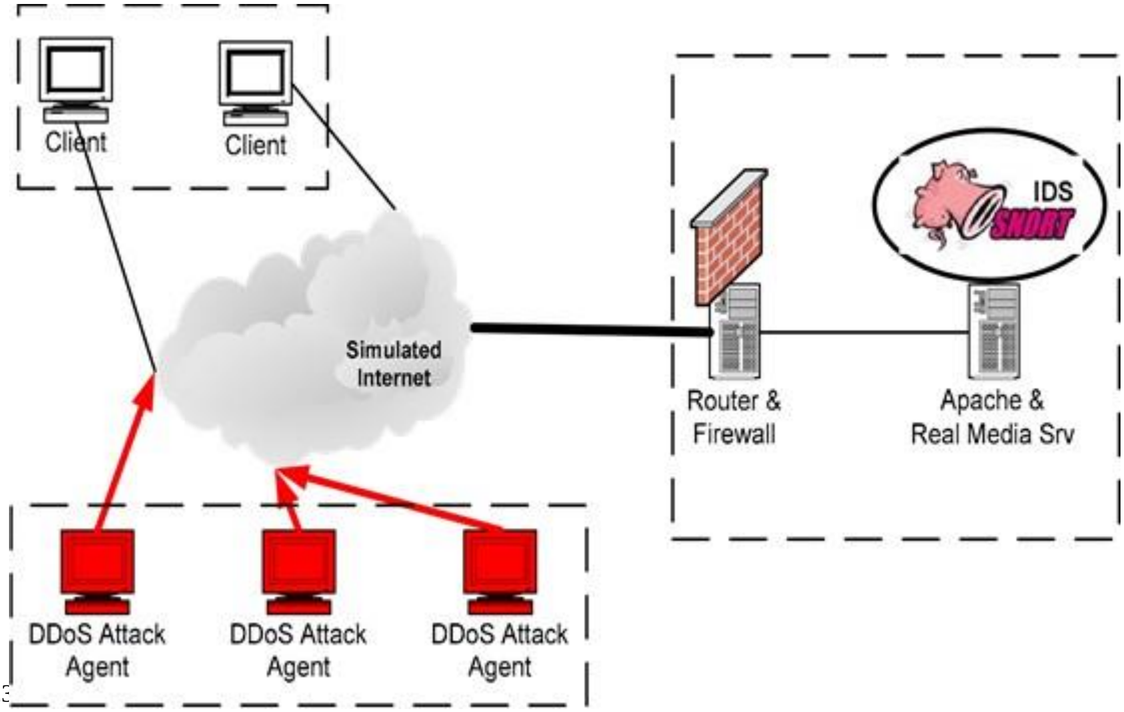
Figure 8: Apply the policy for VPN



□	Name	Default Action	Reporting	Description	Manage
□	Allow All	Allow	Enabled	Allow all Internet Access	
□	Allow yammer	Allow	Enabled		
□	BlockFacebook	Allow	Enabled		
□	CIPA	Allow	Enabled	Internet Access Policy for Children's Internet Protection Act	
□	Deny All	Deny	Enabled	Deny Internet Access	
□	Facebook Allowed Web Policy	Allow	Enabled		
□	Goosip Block	Allow	Enabled		
□	Inda Web Policy	Allow	Enabled		
□	Server Web Policy	Allow	Enabled		
□	Standard Web Policy	Allow	Enabled		
□	Technical IP	Allow	Enabled		
□	Testing Web Policy	Allow	Enabled		
□	YouTube Allowed	Allow	Enabled		

Figure 9: Web Filtering

Therefore the variation of known-attacks are not fully detected by the Firewall. The most general signatures have very high network traffic to provides false alert by systematically implementing generalized rules and alerts [15],[16].



Copyright ⓒ2020 SERSC

Figure 10: Snort IDS put front of the Firewall

Above Figure shows the test bed built for the DDoS attack, detection and defense simulation Snort IDS put front of the Firewall, or keep the Snort IDS in between Firewall and internal network [1],[2],[17],[18]. Because the best solution must be the below Figure it has shown protect internal network and which the intrusion coming through the Firewall. Regular and systematic reviews of firewall policies should be put in place[19],[20]. These reviews provide important benefit, mitigating challenges such as:

1. Mistakenly adding duplicate, similar, or overriding firewall policies.
2. Missing the impact of corporate policy changes that may impact particular rules.
3. Creation of policies that too specific at the time implementation and may need to be broadened to be effective.
4. Determining when policy should be implemented.

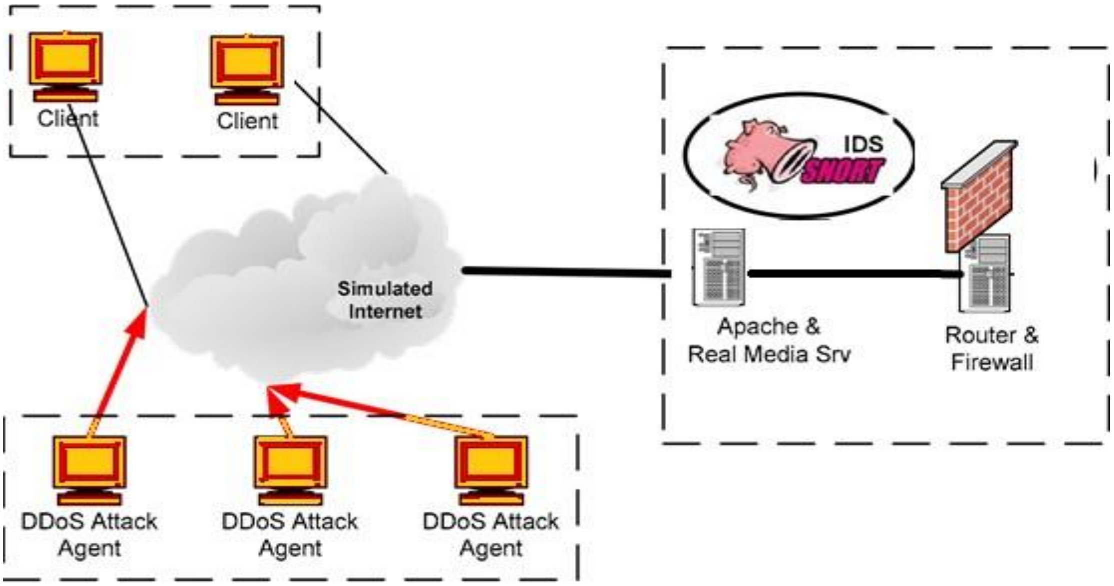


Figure 11: Snort IDS in between Firewall and Internal Network

The TCP/IP over the Ethernet shows the SNORT sensors consider the cloud attacks [7], [8]. THE Span is the most important traffic routers to gives mirror to aggregates the only one interface that will not at all transmit [21].

VII. CONCLUSION

The curb based incidents , the security challenges are plays a vital role are become most common. The network users are in the corporate world to become the most needed role in IDS tool. Some sellers are selling a diagnostic system used by artificial intelligence (AI) to find out the goals. Network The most efficient part of the IDS digital network, known as the IDS node, is protected by every host in the network. However, there are still many challenges to overcome. Improving, mining, and reducing data is critical to keep in touch with various building blocks in the future. Undoubtedly, rapid and dynamic screening techniques are necessary to detect the various intelligent and unusual attacks we encounter. Finally, co-operation with not only the IDS, but also with other network security entities, is an obligation to achieve a comprehensive network security environment for future organizations.

REFERENCES

[1] F. Anjum, D. Subhadrabandhu and S. Sarkar. Signature based intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[2] D. E. Denning, An Intrusion Detection Model," IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222- 232, USA, 1987.

[3] Herve Debar. (April 29th-May 1st, 2000) *“An Introduction to Intrusion-Detection Systems”*, In Proceedings of Connect’2000, Doha, Qata.

[4] DDoS Attack https://www.flowmon.com/en/solutions/use-case/ddos-protection cited October 2018.

[5] DDoS Attack https://www.symantec.com/connect/articles/barbarians-gate- introduction-distributed-denial-service-attacks cited October 2018.

[6] B. S. Kiruthika Devi, G. Preetha, G. Selvaram and S. Mercy Shalinie, "An impact analysis: Real time DDoS attack detection and mitigation using machine learning," 2014 International Conference on Recent Trends in Information Technology, Chennai, 2014, pp. 1-7. doi:10.1109/ICRTIT.2014.6996133.

[7] Karthick, R: “A Reconfigurable Method for Time Correlated Mimo Channels with a Decision Feedback Receiver,” International Journal of Applied Engineering Research, 12 (2017) 5234.

[8] Irom Lalit Meitei, Khundrakpam Johnson Singh, and Tanmay De.2016. Detection of DDoS DNS Amplification Attack Using Classification Algorithm. In Proceedings of the International Conference on Informatics and Analytics (ICIA-16). ACM, NewYork, NY,
USA, Article 81, 6 pages. DOI: https://doi.org/10.1145/2980258.2980431.

[9]G. Ramadhan, Y. Kurniawan and Chang-Soo Kim, "Design of TCP SYN Flood DDoS attack detection using artificial immune systems,"2016 6th International Conference on System Engineering andTechnology (ICSET), Bandung, 2016, pp. 72-76. doi:10.1109/ICSEngT.2016.7849626.

[10] Karan Singh, R. S. Yadav, Ranvijay International Journal of Computer Science and Security, Volume (1): Issue (1) 56.

[11] Vedavathi, T. and Karthick, and P, Meenalochini, Data Communication and Networking Concepts in User Datagram Protocol (UDP) (January 22, 2020). Available at SSRN: https://ssrn.com/abstract=3523820 or http://dx.doi.org/10.2139/ssrn.3523820

[12] Paul Innella and Oba McMillan, Tetrad Digital Integrity, LLC “An Introduction to Intrusion Detection Systems” December 6, 2001.

[13] Micheal E. Whitman and Herbert J. Mattord, “Principles of Information Security” page 289-294.

[14] Karthick, R: “Design and Implementation of Low Power Testing Using Advanced Razor Based Processor,” International Journal of Applied Engineering Research 12 (2017) 6384.

[15] Christos Douligeris and Dimitrios N. Serpanos “Network Security Current Status and Future Trends”.

[16] Varun Chandola, Arindam Banerjee, and Vipin Kumar“Anomaly Detection: A Survey” August 15, 2007.

[17] Abouabdalla, O., H. El-Taj, A. Manasrah and S. Ramadass, 2009. False positive reduction in intrusion detection system: A survey. IEEE: pp: 463-466.

[18] Agarwal, P., P. Yadav, N. Sharma, R. Uniyal and S. Sharma, 2012. Network security is a key for internet users: A perspective. Indian Journal of Engineering, 1(1): 92-95.

[19] Karthick, R : “A novel 3-D-IC test architecture-a review,” International Journal of Engineering and Technology (UAE),7 (2018) 582.

[20] Alharby, A. and H. Imai, 2005. Ids false alarm reduction using continuous and discontinuous patterns. Springer: pp: 423-442.

[21] Karthick, R: “PSO based out-of-order (ooo) execution scheme for HT-MPSOC”, Journal of Advanced Research in Dynamical and Control Systems, 9 (2017) 1969.