International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.5, February 2016 – www.ijais.org

Intrusion Detection System for DoS Attack in Cloud

Mishti D. Samani
M.Tech Student
Dept. Of Computer Science and Engineering
Nirma University
Ahmedabad-382481
Gujarat, India

Miren Karamta
Bhaskaracharya Institute for Space Applications and Geo-Informatics
Gandhinagar-382007
Gujarat, India

Jitendra Bhatia
Faculty of Computer Science and Engineering
Nirma University
Ahmedabad-382481
Gujarat, India

M.B. Potdar
Bhaskaracharya Institute for Space Applications and Geo-Informatics
Gandhinagar-382007
Gujarat, India

ABSTRACT
Open and distributed nature of cloud, vulnerability of internet, different limitations of cloud service models are some of key features for the attraction of various attackers. One of the security concern for cloud is denial of service attack. Due to effect of this attack, legitimate users request are not processed. A Defense mechanism is required to secure network from such sophisticated attacks. Intrusion detection is mainly used to identify attacks and log the reports. Intrusion detection system is proposed based on knowledge multi-threaded system. Single technique is not sufficient enough to detect such attacks. Multithreaded knowledge based IDS has been proposed to detect DOS attacks.

Keywords
Cloud computing, sophisticated attacks, multithreaded, anomaly detection, firewall, DDOS, SaaS, PaaS, IaaS.

1. INTRODUCTION
Cloud computing is popular due to its numerous characteristic and benefits. Reduction of Cost, Scalable and flexible, Quick and Easy implementation, Reduced Maintenance cost, Quality of Service, Mobility and so on has advantages has made cloud popular in small and large scale industries. We have been dependent on cloud technologies such as Google docs, amazon's storage cloud, Dropbox, Skype and so on applications. In spite of its numerous advantages it faces numerous security challenges such as security and privacy, loss of control and lack of standards.

There are five essential characteristics:

1. Resource Pool

Computing Resources such as Processing Power, network bandwidth, and memory and storage area must be in virtualized into some virtualized pool can be allocated dynamically based on end user demands.

2. On-Demand service

There is no need of any human intervention and provider to access server time and network storage.

3. Regular Service

It provides the facilities of resource monitoring, controlling, reporting usage of amount resources and this can be served to users.

4. Rapid Elasticity

Services provided to end-users are unlimited and provided based on their request.

5. Wide Network Accessibility

Services can be accessible on various devices such as mobile phones, tablets, laptops, workstations.

Models and its Limitations

1) INFRASTRUCTURE-AS-SERVICE: This model is also well known as self-service model. This models offers computing resources such as virtual server space, accessing and monitoring network connection, load balancers, bandwidth, storage devices , security and IP addresses in virtualized environment. Own platforms can be built by client as they are provided with facilities of accessing virtual components. Services provided are virtual server and cloud storage. Some of its limitations are: It is mainly dependent on security features provided by the cloud service provider. It is vulnerable to DDoS, connection flooding, Impersonation, Disrupting communication and Defacement.

2) PLATFORM-AS-SERVICE: This model delivers applications over the internet. PaaS provider host hardware and software on its own infrastructure. Services provided are runtime environment for application code, cloud storage and other services such as Integration. Some of its limitations are: It is vulnerable to side channel attacks, cross site scripting, password reset attacks, social engineering attacks, and brute force attack. It is also more vulnerable as insecure permissions are granted on cloud data. It is necessary even to protect API keys. It is difficult to integrate with the rest of the system. It is unable to protect private information before uploading cloud data by means of encryption. Some of the default configuration of applications is vulnerable to attack.

3) SOFTWARE-AS-SERVICE: In this service model, End user is consumer. Services provided is for end application. Some of its limitations are: Authentication weakness, Session management weaknesses, Buffer overflow, DoS attacks are some of the challenges faced by SaaS. Some of the limitations related to data security are cross site scripting, OS and SQL injection flaws, Insecure storage and configuration, cookie manipulation, access control weakness. Insecure session management, data validation, SQL injection flaws, network penetration and packet analysis, IP spoofing are some of limitations.

2. BACKGROUND
2.1 Intrusions in Cloud Environment
Different security attacks are performed with different motives and they corrupt the system in different ways. These vulnerabilities results in violations of different properties: Availability, Confidentiality, Integrity and Control.

Some of the intrusions can affect availability, confidentiality and integrity. They are [3]:

1) Insider Attack
An authorized users tries to gain a higher privileged levels. Sometimes they may even disclose secret information of the organization. Such attacks are carried by employees of the organization.

2) Flooding Attack
Attacker sends huge number of packets of TCP, UDP, ICMP or mix of them by flooding the victim. Illegitimate network connection is responsible for the attacks. In cloud, VM is open to internet so there is high risk of DoS (or DDoS) through zombie. [3]

It mainly affects service availability which leads to loss of availability of resources to the intended or authorized users. It will completely exhaust hardware devices and would no longer able to carry out intended tasks.

3) User to Root Attack
Attacker tries to gain authorized access by sniffing the password. This would further be used to exploit vulnerabilities of root level access. Such attacks takes place when static buffer is overfilled. Some security risks such as password recovery workflows, phishing attack, key loggers etc. don't possess any standard mechanism to prevent security risks. In cloud, attacker tries to gain valid user instances via to obtain root level access of VM.

4) Insider Attack
An authorized users tries to gain a higher privileged levels. Sometimes they may even disclose secret information of the organization. Such attacks are carried by employees of the organization.

5) Flooding Attack
Attacker sends huge number of packets of TCP, UDP, ICMP or mix of them by flooding the victim. Illegitimate network connection is responsible for the attacks. In cloud, VM is open to internet so there is high risk of DoS (or DDoS) through zombie. [3]

It mainly affects service availability which leads to loss of availability of resources to the intended or authorized users. It will completely exhaust hardware devices and would no longer able to carry out intended tasks.

6) User to Root Attack
Attacker tries to gain authorized access by sniffing the password. This would further be used to exploit vulnerabilities of root level access. Such attacks takes place when static buffer is overfilled. Some security risks such as password recovery workflows, phishing attack, key loggers etc. don't possess any standard mechanism to prevent security risks. In cloud, attacker tries to gain valid user instances via to obtain root level access of VM.

7) Port Scanning
Various port scanning techniques are TCP Scanning, UDP Scanning, SYN Scanning, FIN Scanning, ACK Scanning, and Window Scanning. They lists various open ports, closed ports and filter ports. Various Information such as IP address, MAC address, router, gateway filtering, firewall rules and so on can be known and can be misused.

8) Attack on virtual machine or hypervisor
To gain a complete control over virtual machine, the lower layer needs to be compromised. Some of popular attacks on virtual layer are BLUEPILL (2006), SubVir (2006) and DKSM are some well-known attacks on virtual layer.

Zero Day vulnerabilities are found in VM to gain complete access. A zero-day vulnerability was exploited in hyperVM virtualization application which resulted in destruction of many server based websites (2009). [2]

9) Backdoor Channel Attacks
Hacker gains remote access in infected code by compromising confidentiality. Thus it is a passive attack that can control victim's resources and use it as zombie to perform DDoS attack. Attacker can get access and control of cloud user resources by compromising the system. To prevent such attacks firewall, signature and anomaly based intrusion detection system is used.

2.2 Intrusion Detection System

Framework for intrusion detection system is represented fig 1.

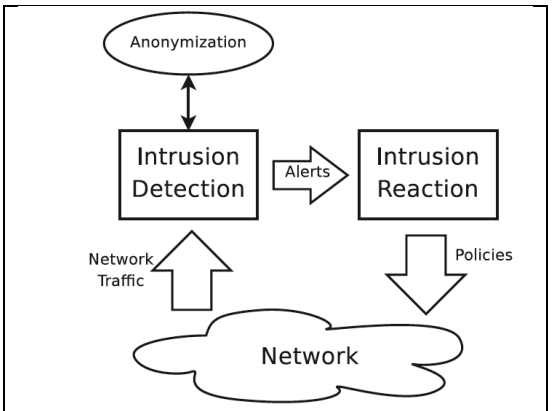

Fig 1: Macro components positioning within the system frameworks [14]

Three main Components of IDS are as follows:

1) Intrusion detection system
To classify anomalous traffic summarization algorithm and pattern recognition techniques are used.

2) Anonymizer
Some real life traces such IP addresses, application information are used to train the pattern recognition algorithm.

3) Intrusion Reaction system
Alert signals acts as triggers for information exchange and trace back the attack resources.

Above architecture is dependent on classical IP Infrastructure.

Framework for Intrusion Detection System

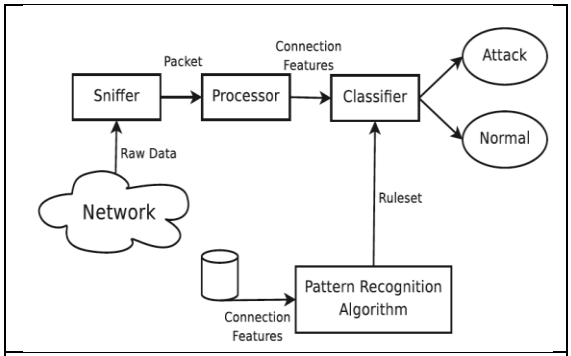

Fig 2: Framework for Intrusion Detection system

Model is composed of two parts:

1) Real time Intrusion Detection system
It is based on user behavioral model network packets are analyzed and classified.

2) Pattern Recognition System
Data from user behavioral model is extracted and stored in database along with network traffic features and pattern recognition algorithm.

Types of Intrusion Detection System
Intrusion can be of several types such as: Attempted Break-ins, Masquerade attack, Penetration testing, leakage, Denial of Service, Malicious use.

There are six different Intrusion Defense Solutions:

1) Based on approach used
a) Intrusion Detection System

It Detects vulnerabilities at host and network layer. Its main function is to alert the system.

b) Intrusion Prevention System

Its main characteristic is sending alarm, dropping malicious packets, blocking traffic.

Its main function is to prevent detected attack. Some of its limitations are Conceptual issues (Packet alteration), signature issues, Hardware Issues. Signals false alarms.

c) Intrusion Response System

It will respond once alert is raised. It responds in an automated manner in which it is defined. One of its limitation is Lack of evaluation of response cost.

d) Intrusion Tolerance System

Classical fault tolerant techniques and error hiding techniques are applied. The main mechanism is to prevent system from security failure.

2) Modules of Defense system
a) Monitoring

It is State of network, traffic analysis are monitored. It is Collection of traffic characteristics.

b) Detection

It is used to identify intrusions, logging information & reporting attempts. The main function is to analyze various area of network to identify misuse and intrusions.

c) Reaction

It Possess active and passive component. It displays the alert, logging events or paging administration.

3) Based on nature of control
a) Centralized

It Produces alerts locally. It handles high amount of data in short period of time. Central unit is crucially vulnerable, any failure in central server collapse whole process.

b) Hierarchical

At lowest layer of IDPS detection is done. Detection element and event correlation handler is detected at higher level. It is more scalable then centralize unit. It suffers from vulnerability of central unit.

c) Distributed

It is fully autonomous distributed controlled system. During decision making information is not available. Alert possess single feature for detection of attack. Accuracy is reduced, hard to detect attacks as it's too narrow.

4) Based on Defense Infrastructure

a) Host-Based

It Protects from buffer overflow attacks and enforces security policy It Monitors the dynamic behavior inform of anti-virus packages. One of its limitations Host server is compromised by an attack.

b) Network-Based

Analysis of user behavior, detection of worms, viruses & security hole. It Enforces security policies. Some of its limitations are: High false positive, performance issues, encryption, new and sophisticated attacks, human intervention, and evasion of signature. Some of attacks detected: Scanning attack, Denial of Service, Penetration attacks.

5) Defense Location

a) Victim-end defense mechanism

It is employed at routers on victim side. High resource consumption due to victims end. It Detects attacks only after it reaches victim and legitimate clients are affected.

b) Intermediate network defense mechanism

It Maintains detection accuracy and attack bandwidth consumption. It Cover source and victim end. All router should apply this detection scheme to avoid failure.

c) Source-end defense mechanism

It Prevents congestion on whole network. It is practically impossible to deploy. Some of its Limitations are: Platform flexibility, host can be easily compromised, inability to correlate.

6) Based on technique used

a) Misuse Detection

It is Based on the matching the sequence of signature action. Explicit knowledge of the attack is required for its detection. It Detects pattern of known attacks more accurately. It cannot detect unknown attacks

b) Anomaly Detection

It statistically measure the system features. It consist of Training Phase: Normal traffic profile is generated, Anomaly detection: learned profile is applied to current traffic

OVERVIEW OF IDS TECHNIQUES

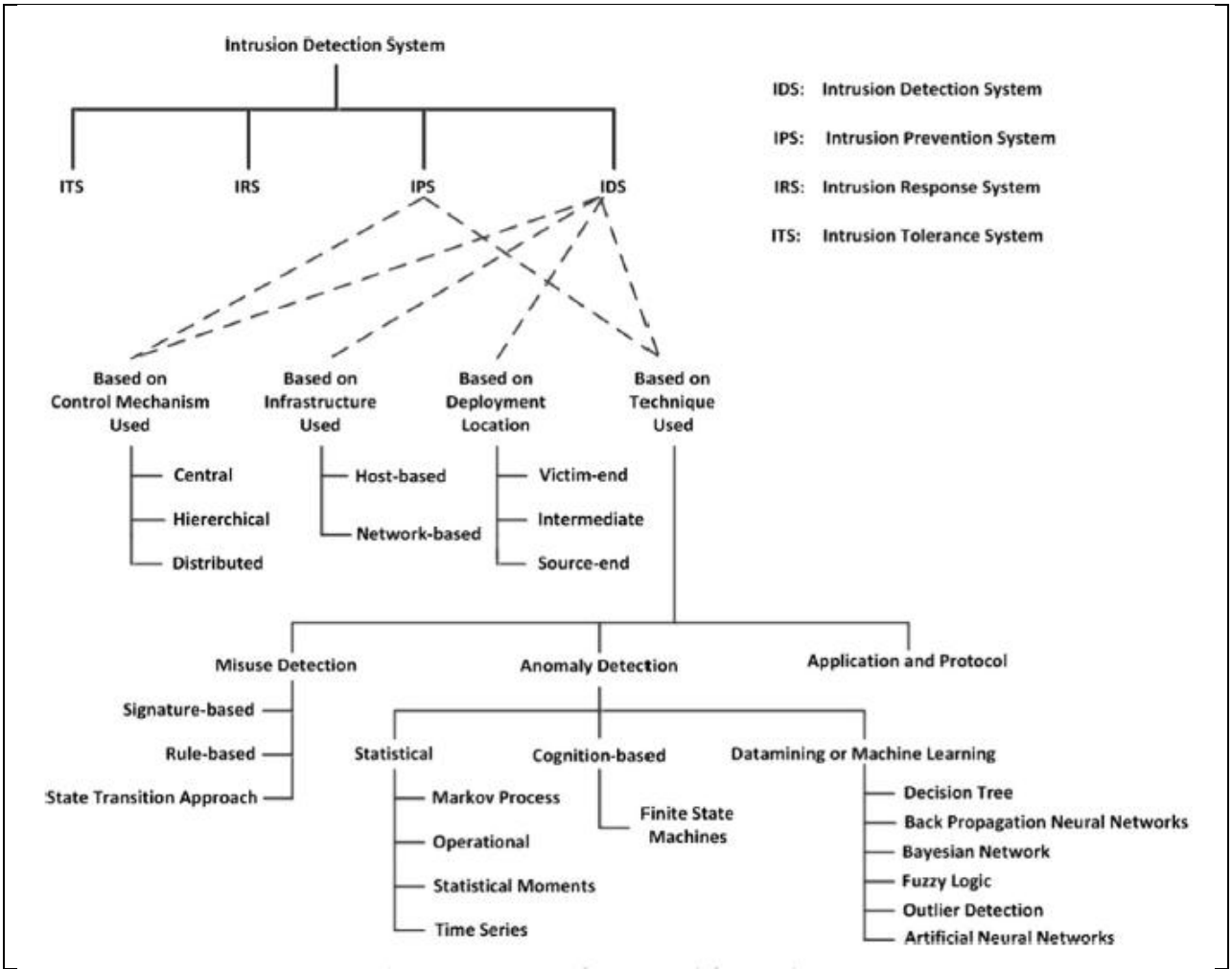

Fig 3: Overview of IDS techniques [6].

COMMONLY DETECTED ATTACKS BY IDS

IDS reports three types of attacks:

1) System Scanning

System scanning can take place when attacker sends different kind of packets to the target network. Based on response from target, systems characteristics and vulnerabilities can be discovered.

These attacks are passive in nature and do not compromise or penetrate systems. Some of tools to perform scanning attacks are: Port Scanner, Network Scanner, Port mapper, Network Mapper, Port Scanner or vulnerability Scanner.

Different Characteristics of system that can be exhibited by this attacks are:

- Target networks topology
- Number of Active host on network
- Server software running on network
- Software Version numbers
- Operating system that hosts is running

This scanners discover for specific vulnerabilities. While attacker can run a vulnerability Scanner, it will output list of hosts that are vulnerable to specific attacks. Thus attacker can use this information to launch a real attack. IDS should be able to differentiate between legitimate and malicious scanning. Users that are connected to Internet are almost scanned. Scanning attack is the most common attack that can cause serious penetration attempt.

2) Denial of Service

In today's generalization, dos attack are very common. It attempts to slow or shut down target systems or networks. This attacks is performed with different motives. DoS attack incurred major losses in electronic commerce operations as many of users where unable to access them at the time of purchase. There are two types of DoS attacks:

3) Flaw Exploitation DoS attack

It is also known as Ping of Death attack. It mainly exploits flaw in software of target system causing processing failure or exhaust system resources. In this type of attack, large ping packets are send to target system. Target System cannot manage such abnormal packets resulting into the system crash. Different targeted resources are CPU time, memory, disk space, space in a special buffer, network bandwidth.

Different possible methods of DoS attacks is to exhaust resources of IDS. It would flood IDS with traffic that

generates alerts until IDS run out of resources. Thus it would generate incomplete log of events.

4) Flooding DoS attack

The target is flooded with information more that can it handle. Target System cannot be patched when system is under this attack. Several Modification techniques can be used to mitigate such attacks. DDOS are flooding dos attack where multiple users are used to launch the attack. They are centrally controlled and acts as single immense system. Thus, fastest system can be bring it to halt.

5) System Penetration

Unauthorized Acquisition or system privileges, resources or data are involved in system penetration. Various software flaws are exploited to gain control of a system. Their details and impact vary.

Different types of system penetration are:

a) User to Root:

Target host is completely controlled by local user.

b) Remote to User:

An account of target host is managed by the attacker on the network.

c) Remote to Root:

Target host is completely controlled by the attacker on the network.

d) Remote Disk Read:

An ability to read private data files on target host without authorization of owner by an attacker on network.

e) Remote Disk write:

An ability to write private data files on target host without authorization of owner by an attacker on network.

DENIAL OF SERVICE

Dos attack can cause some of problems such as Ineffective services, inaccessible services, Interruption of network traffic in connection interface.

Following are the ways to identify DoS attacks:

- unusually slow network performance
- unavailability of particular site
- increase in time span to access your account
- inability to access website

According to Prolexic Q1 2014 Global attack report, DOS attacks has increased by 18% in US. Most Vulnerable and popular protocols that are targeted are Character Generation Protocol (CHARGEN), Network Time Protocol (NTP) and Domain Name System Protocol (DNS) that can be easily hide source attack and identity. At infrastructure level more than 87% attacks take place. So DoS attack is vulnerable at Infrastructure level.

MODES OF ATTACKS

Denial-of-service comes in various forms and services. There are three types of attack:

1) Consumption of Scarce , limited or non-renewable resources

Some of things such as network bandwidth, memory, disk space, CPU time, data structures, access to computers and networks and other environmental resources.

2) Network Connectivity

DoS attack mainly takes place in network connection. Example of this type of attack is "SYN Flood".
Attacker's machine has established connection with the victim machine such a way that connection is half open. Victim machine reserves limited number of data structures which requires to complete the connection. This attack results in denying of legitimate connections leaving half open connections. Kernel level data structure is been consumed by the intruder.

3) Using your own resources against you

Usage of individual's own resources is been exploited by intruder in unexpected ways. Intruder uses forged UDP packets by connecting to echo service of one machine to another. This results in complete consumption of network bandwidth between them.

4) Bandwidth Consumption

A large number of packets of ICMP ECHO is been directed to the network resulting into the consumption of network bandwidth.

5) Consumption of other resources

Intruders may consume some other resources that are necessary for system operation. Example, Limited data structures are available to hold the process information such as identifiers, entries and process slots. It may be just created by writing the script that copies itself. This can be sometimes prevented by the quota facilities provided by the operating system. If the table is not filled by copying the scripts then CPU may consume large number of processes and associated time between switching.

Even disk space is consumed in numerous ways:

- Generation of excessive mail messages
- Placing files in anonymous ftp areas or network shares
- Intentionally generating errors that are already logged.

If there is no bound on amount of data written on disk it can lead to denial of service. This may even cause system crash or may become unstable by sending malicious data over network.

The attack is likely to take place once system faces frequent crashes with no specific cause. Some of things that are vulnerable to dos attack or can be used in malicious way are: printers, tape devices, network connections, and other limited resources.

TYPES OF DOS ATTACKS

Different types of dos attacks are:

1) Application Layer Attack

The main aim is to flood server with large number of request with resource handling and processing. Examples of such

attacks are, HTTP Floods, DNS query flood attacks and slow attacks.

2) Network Layer Attack

They mainly aim to exhaust network resources. Examples of such attacks are UDP Flood, SYN Flood, NTP Amplification and DNS amplification attacks. 20 to 40 Gbps traffic events are enough to shut down network resources.

3) Buffer overflow Attack

The attacker would exploit the vulnerability by sending the large amount of data it can handle. Some of its characteristics are: Sending large number of ICMP messages, sending emails with 256 characters to netscape and Microsoft mail messages.

4) Smurf Attack

In this type of attack, a large number of ICMP packets are broadcasted to a computer network with victim's spoofed source IP address. With this flooding, spoofed host will not be able to distinguish or receive real traffic.

5) SYN Attack

A limited buffer space exists for the rapid hand shaking of messages by setting up sessions. This packets consists of sequence number for exchange of messages. A large number of packets are send and then not responded leaving large number of packets in buffer not permitting the legitimate requests.

6) **Teardrop Attack**

The IP Protocol packets are divided into fragments. This packets are identified by the offset at the beginning of packets. The attacker puts a confusing value to the second or later fragments, which leads to system crash.

7) Viruses

The viruses replicate across a network in various ways where a host is targeted. In such attack depends on severity, attacks can be hardly noticed.

8) Physical Infrastructure attacks

Snipping of fiber optic cable is included in it. Such attacks can be mitigated by rerouting the traffic.

MITIGATIONS OF DOS ATTACKS
Various mitigation techniques are as follows:

- Purchase lot of bandwidth which will make hard for attacker to clog the network.
- Use of Intrusion prevention system and firewall can limit dos attacks.
- Use of throttling and rate-limiting technologies can reduce dos effects.
- Ingress and Egress filtering: A valid source address will be allowed to enter and leave the packets [8].
- Filtering packets based on route information by preventing spoofed packets from Spoofed address [8].

2.3 EXISTING IDS

Following are the existing IDS for dos attack detection:

- Multithreaded IDS have been proposed for the distributed system. It is mainly used to detect masquerade attacks, host and network based attacks [18].
- Jabez suggested an approach to use the outlier detection for the network intrusion detection system [9]. The paper focused on little variation of attacks, low false alarm rates.
- Narwane proposed knowledge and behavior based approach to detect anomalies. Behavior of system is observed and slight change in behavior will trigger the alarm and if changed behavior remain unnoticed then network packet is been compared with database of vulnerabilities which will raise an alert [17].
- Bamakan demonstrated two methods name multiple critical linear programming and swarm particle optimization to improve performance by decreasing false alarm rate [10].
- Another approach is network based signature which is placed at each node to detect SIP flooding attack [20]. Modi has even proposed hybrid technique to detect major attacks and should be located at server [3].
- Hybrid technique of two approach covariance matrix based and entropy based system has been proposed [22].

2.4 2.3LIMITATIONS OF IDS

Limitations of IDS with respect to DoS attack are as follows:

- Evasion of signature can be critical threat.
- Traffic audit data changes with time interval making it difficult differentiate normal traffic from anomaly [5].
- They cannot hide security vulnerabilities in network protocols.
- NIDS cannot even determine whether an attack was successful.
- It's significantly error prone i.e. more number of false positive [17].
- Monitoring user behavior is difficult [17].
- Human intervention is always required and it always looks for known pattern or behavior.
- Timer increases as double check points are kept so it degrades the performance [22].
- Difficult to detect unknown and novel attacks, requires huge execution time and is less accurate [9].
- IDS cannot be complete reliable solution against security threats.
- Encrypted packets are not processed which can cause intrusions in network.
- Complexity increases as more number of techniques are combined [3].

2.5 PROPOSED WORK

To Detect DoS attack, single method is not completely reliable. Combination of different techniques is used. Different ways are monitor network resources, File system usage, Detection using snort, Rule based DoS attack detection and Fuzzy logic to determine the severity.

With the changing behavior of internet it is mandatory to monitor the network and maintain system monitoring logs. Administer should be notified once malicious traffic are detected. One of the way to detect DoS attack is to identify usage of system resources such as Number of users logged in, System uptime and load time, free and used memory, memory consuming process, architecture and operating system is shown in figure 4. It is also necessary to scan the request by limiting the rate of incoming request and updating the local database is shown in figure 5. Even load time, bandwidth consumption, scanning the network and bandwidth consumption can also be known.

Even the memory usage can be obtained in html form. All the details can be obtained and can be scheduled using crontab based on the requirement. This details can be obtained through mail and alerts. This details of memory and CPU usage is one of the way to detect the DoS attack by analyzing the file system and time consuming process. This usage of resources can be known by monitoring the system is shown in figure 6. Even the process that consumes maximum memory can also be determined. This can be scheduled at regular time intervals and based on that alerts can be generated by determining the threshold value.

Snort is an open source Intrusion detection System. Snort is configured to detect DoS attack. This attack can be even detected in the graphical form. BASE (Basic Analysis and Security Engine) provides functionality of graphical interpretation of DoS attack. The implementation is carried out in Ubuntu 15.04 along with Barnyard2 2-1.13, pulled pork 0.7.0 and BASE 1.4.5. System monitoring would be continuously running in background and would send alert report to the administrator. One such example is, Figure 7 represents TCPSYN flood attack can be detected by snort and can be represented in BASE.

Another technique that is proposed is a multithreaded signature based fuzzy logic based system is proposed. This fuzzy logic contains the classifiers to detect the severity of attack. The severity of attack determines the alert rate. This classifiers contains the expert or knowledge based rules to determine the severity. It may happen that some of attack may last for some minutes to some hours. It tries to detect possible known DOS attacks with the help of signature patterns and expert rules. The accuracy and performance is dependent on expert rules. This system would continuous monitor the network packets and based on severity of attacks, alerts would be generated. It will even scan the system looking for the other vulnerabilities and loop holes. The vulnerabilities of web applications would be scan and would be notified accordingly. Knowledge based approach is used so that accurate results can be obtained. However it is difficult to detect variation of attacks unless expert rules are made such. Every time data containing packets signature are matched with the dataset containing patterns. Some rules are defined to find out malicious characteristics. This set of rules are stored in database containing information about the pattern. With each novel attack, database can be updated.

3. CONCLUSION

The proposal of an Intrusion detection system for DoS attack in cloud is been made so that there can be minimization of cyber-attacks. NIDS should be incorporated at infrastructure layer. To conclude aim is to reduce impact of dos attack by detecting it at initial state with improved accuracy so that accordingly actions can be taken. NIDS will detect the events based on rules and would alert the security administrator. Monitoring System resources and file system , Detection using rule based algorithm and Fuzzy logic to determine the severity of attack are some of the methods to detect DoS attack. This method are combined to form a reliable solution. Fuzzy model can be updated by updating signatures and can be used effectively to detect known attacks.

4. REFERENCES

[1] Rajendran, Praveen Kumar, B. Muthukumar, and G. Nagarajan. "Hybrid Intrusion Detection System for Private Cloud: A Systematic Approach." *Procedia Computer Science* 48 (2015): 325-329.

[2] Choo, Kim-Kwang Raymond. "Cloud computing: challenges and future directions." (2010):

[3] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan. "A survey of intrusion detection techniques in cloud." *Journal of Network and Computer Applications* 36, no. 1 (2013): 42-57.

[4] Patel, Ahmed, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino Júnior. "An intrusion detection and prevention system in cloud computing: A systematic review." *Journal of Network and Computer Applications* 36, no. 1 (2013): 25-41.

[5] Deka, Rup Kumar, Kausthav Pratim Kalita, D. K. Bhattacharya, and Jugal K. Kalita. "Network defense: Approaches, methods and techniques." *Journal of Network and Computer Applications* 57 (2015): 71-84.

[6] Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." *Information Sciences* 305 (2015): 357-383.

[7] Deshmukh, Rashmi V., and Kailas K. Devadkar. "Understanding DDoS Attack & its Effect in Cloud Environment." *Procedia Computer Science* 49 (2015): 202-210.

[8] Jabez, J., and B. Muthukumar. "Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach." *Procedia Computer Science* 48 (2015): 338-346.

[9] Hosseini, BS Mojtaba, Behnam Amiri, Mahboubeh Mirzabagheri, and Yong Shi. "A New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming." Procedia Computer Science 55 (2015): 231-237.

[10] Che, Jianhua, Yamin Duan, Tao Zhang, and Jie Fan. "Study on the security models and strategies of cloud computing." Procedia Engineering 23 (2011): 586-593.

[11] Fatema, Kaniz, Vincent C. Emeakaroha, Philip D. Healy, John P. Morrison, and Theo Lynn. "A survey of Cloud monitoring tools: Taxonomy, capabilities and objectives." Journal of Parallel and Distributed Computing 74, no. 10 (2014): 2918-2933.

[12] Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36, no. 1 (2013): 16-24.

[13] Di Pietro, Roberto, and Luigi V. Mancini. Intrusion detection systems. Vol. 38. Springer Science & Business Media, 2008.

[14] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583-592.

[15] Narwane, S. V., and S. L. Vaikol. "Intrusion Detection System in Cloud Computing Environment." In InInternational Conference on Advances in Communication and Computing Technologies (ICACACT). 2012.

[16] Mohod, Akash G., and Satish J. Alaspurkar. "Analysis of IDS for Cloud Computing." International Journal of Application or Innovation in Engineering & Management (IJAIEM) Vol 2: 344-349.

[17] Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34, no. 1 (2011): 1-11.

[18] Mazzariello, Claudio, Roberto Bifulco, and Roberto Canonico. "Integrating a network IDS into an open source cloud computing environment." In Information Assurance and Security (IAS), 2010 Sixth International Conference on, pp. 265-270. IEEE, 2010.

[19] Kene, Snehal G., and Deepti P. Theng. "A review on intrusion detection techniques for cloud computing and security challenges." In Electronics and Communication Systems (ICECS), 2015 2nd International Conference on, pp. 227-232. IEEE, 2015.

[20] Girma, Anteneh, Moses Garuba, Jiang Li, and Chunmei Liu. "Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment." In Information Technology-New Generations (ITNG), 2015 12th International Conference on, pp. 212-217. IEEE, 2015.

5. APPENDIX

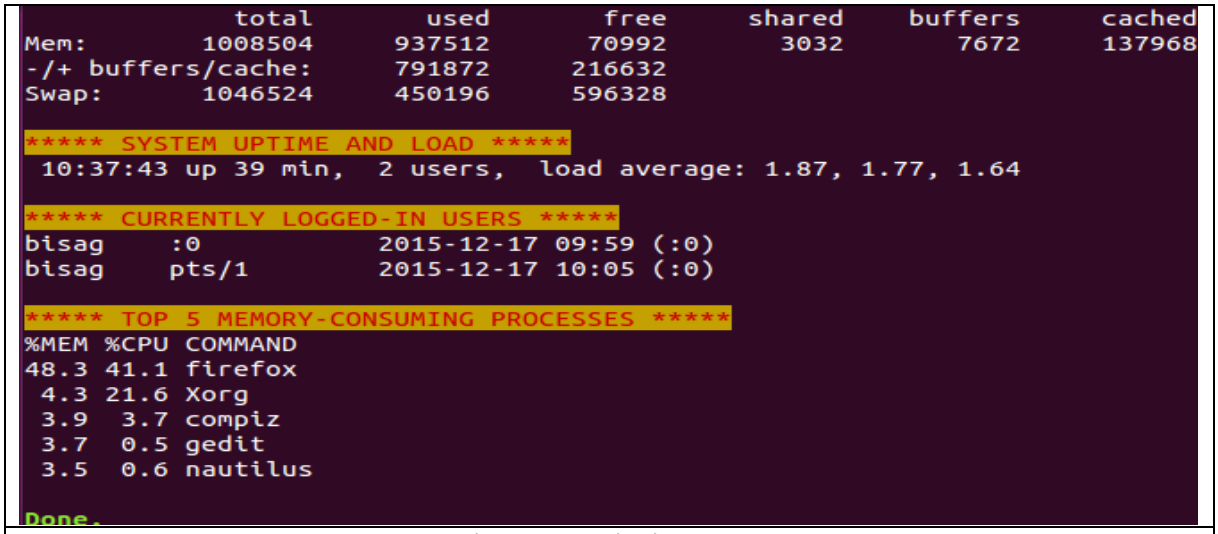

Figure 4 :-Monitoring system

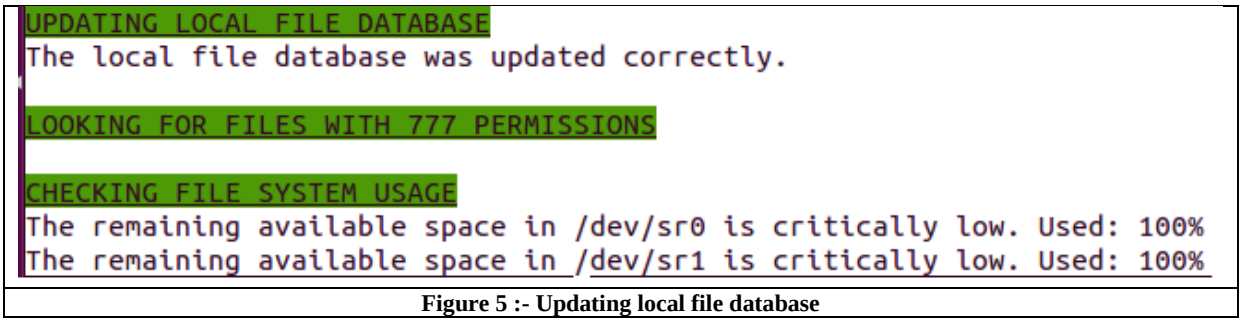

Figure 5 :- Updating local file database

Filesystem usage for host **localhost**
Last updated: **Sun Dec 20 06:07:38 PST 2015**

Filesystem	Size	Use %
udev	482M	0%
tmpfs	99M	10%
/dev/sda1	19G	29%
tmpfs	493M	1%
tmpfs	5.0M	1%
tmpfs	493M	0%
cgmfs	100K	0%
tmpfs	99M	1%
/dev/sr0	43M	100%
/dev/sr1	1.1G	100%

Figure 6 :- File System usage

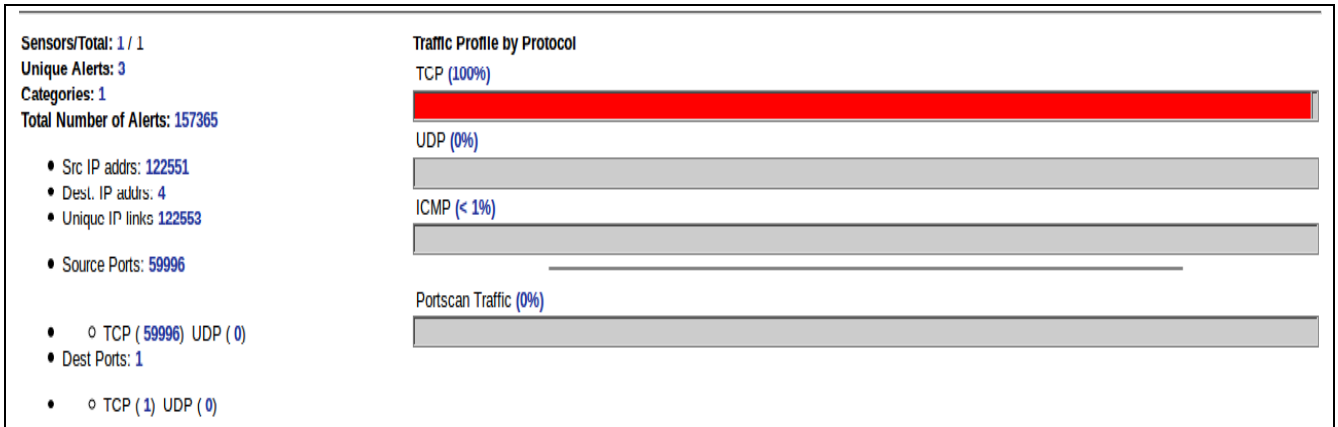

Figure 7 :- Detection of TCPSYN by monitoring TCP traffic using BASE