Adaptive Learning and Automatic Filtering of Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environment

B. S. Kiruthika Devi, T. Subbulakshmi

Abstract: ***Distributed Denial of Service (DDoS) attacks has become the most powerful cyber weapon to target the businesses that operate on the cloud computing environment. The sophisticated DDoS attack affects the functionalities of the cloud services and affects its core capabilities of cloud such as availability and reliability. The current intrusion detection system (IDS) must cope with the dynamicity and intensity of immense traffic at the cloud hosted applications and the security attack must be inspected based on the attack flow characteristics. Hence, the proposed Adaptive Learning and Automatic Filtering of Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environment is designed to adapt with varying kind of protocol attacks using misuse detection. The system is equipped with custom and threshold techniques that satisfies security requirements and can identify the different DDoS security attacks. The proposed system provides promising results in detecting the DDoS attacks in cloud environment with high detection accuracy and good alert reduction. Threshold method provides 98% detection accuracy with 99.91%, 99.92% and 99.94% alert reduction for ICMP, UDP and TCP SYN flood attack. The defense system filters the attack sources at the target virtual instance and protects the cloud applications from DDoS attacks.***

Keywords: DDoS, cloud computing, IDS, virtual instance, detection, defense.

I. INTRODUCTION

Cloud computing model is the most reliable business model due to its various incentives such as availability, scalability, interoperability and flexibility. According to NIST [1], the cloud computing platform conglomerates various resources such as computing elements, network, storage, application and services. The three deployment models are Software as a service (Saas), Platform as a service (Paas) and infrastructure as a service (Iaas). Saas provides the software packages on demand to the cloud users. The software compatibility and the security updates are administered as well. Paas provides the bridging between the infrastructure and software in the cloud environment. It acts as the layer between the hardware and software component. Few popular services of Paas are Google apps and Microsoft azure that helps the cloud users for developing their application on the respective platforms. IaaS provides the resources such as computing device, hardware, network and storage. Without any infrastructure, any user can start a business with minimal risk and high availability of resources. Thus, cloud provides the software, hardware and other computing elements required to run the applications at reduced cost with the aid of these services. Security is the major concern in the cloud computing environment and the risk associated in providing a customizable security model is challenging. Distributed Denial of Service (DDoS) attacks as the one of the top threats in the cloud as listed by the top threats working group [2]. The other threats in the cloud are traffic hijacking, insecure applications, data breach & loss, misuse insiders, shared vulnerability, abuse of service offered by cloud. Distributed Denial of Service attacks (DDoS) is the most important security attack in the cloud computing environment.

The DDoS attackers' motive is to make the critical resources unavailable for legitimate access. The consequences of DDoS attack are service disruption, unavailability of websites, data leakage, reduced productivity, business impact and loss of reputation. The DDoS attack scale has been doubled in 2018 with the increase from 800Gbps to 1.72Tbps. Now, it is expected that the attack scale could be in the levels of terabits since the global IT landscape has vastly expanded [3].

The cloud hosted sites are the major target for DDoS attacks and attackers use sophisticated tools for amplifying the DDoS intensity. DDoS attackers also send ransom notes to the victims and the failure in paying the huge amount of money might deal to data theft, loss of confidential data, high downtime, increased latency, loss of business and loss of data privacy. In the recent years, DDoS attacks are observed in various critical online platforms hosted by private and government organizations.

Popular developer platform was hit by massive DDoS attack with 1.35 terabits of flooding traffic per second. The tracking system detected autonomous system operating at various endpoints. The hosted services by occupy central was exploited by DDoS attack at the rate of 500Gigabits per second. It targeted a mock voting website and news website with seemingly legitimate traffic using botnets.

Revised Manuscript Received on December 04, 2019
***** Correspondence Author
B. S. Kiruthika Devi*, School of Computing Science and Engineering, Vellore Institute of Technology Chennai, TamilNadu, India. Email: kiruthikadevi.bs2015@vit.ac.in
T. Subbulakshmi, School of Computing Science and Engineering, Vellore Institute of Technology Chennai, TamilNadu, India. Email: research.subbulakshmi@gmail.com

The vulnerability in Network Time Protocol (NTP) was exploited to the attacker's advantage to launch a DDoS reflection attack against content delivery provider. It affected many servers in the Europe with the attacking rate of 400Gigabits per second. Threat intelligence organization also experienced DDoS attack using reflection attack with 300 Gigabits of traffic per second. The organization experienced service outage and disruption of business process. Banking websites are also affected by DDoS attacks with peak increase in the traffic level. The attacking rate witnessed at the platform was 60Gigabits per second. Multitude of attacks were launched on the banking sites so that only hybrid/multilevel defense solution can circumvent the massive attack [4].

Cloud computing environment is the major target for cyber attackers since the operating protocols are equally exploited by the attacker inspite of the paradigm shift from the traditional model. The IT/ITES sector depend on the cloud for their business process due to its availability and continued support. Hence, any unpatched component in the cloud network can open door to multiple attacks and to eradicate the DDoS attack becomes critical. Thus, any insecure virtual machine, switch, router or connecting devices can be a prey for DDoS attacks. With the security loopholes, the attackers can deploy malicious program to launch coordinated DDoS attack. The existing cloud service providers provide various solutions such as security application control, authentication, access control, encryption techniques, disaster recovery and risk management [5]. Despite of the solutions available, during multitude attacks protection of cloud is important. Hence, detection of attacks and its variants of DDoS is inevitable in the cloud computing environment.

II. RELATED WORK

Cloud Intrusion Detection System Service (CIDSS) is proposed to secure the cloud clients against cyber-attacks [6]. It is majorly developed for software as a service cloud deployment model. The major components in the CIDSS are Intrusion detection service agent, Cloud Computer Service Component (CCSC) and Intrusion Detection Service Component (IDSC). The first component is the light-weight device that is configured within the end network to capture the network traffic. The agents are put into same/different group based on the ruleset and limit set on the traffic observed in the network. The second component gathers the information from the agents and forwards to the sends to IDSC after formatting the messages. The third component's main functionality is intrusion detection. The engine detects attack with known signature and the alerts are generated by event publisher. DDoS detection model is proposed where the IDS is configured in the virtual switch to analyse the network traffic [7].

The known-attacks are detected with the signature database and the notifications are sent to the server. The packets from the sources that are directly responsible for the attack are dropped by the virtual server. The method could block all the attacker IPs that are causing DDoS attacks and detect such attacks in the virtual environment. But, all the variants of the attacks cannot be detected. Misuse detection using the Snort IDS is developed and implemented in the private cloud Eucalyptus [8]. Snort is configured in the cloud controller and all the host machine. It can detect intrusions originating from the network that are external. This method overcomes the difficulty of deploying the multiple IDS. Since, it is fast and the cost-effective approach it can be deployed on any private/public cloud. However, the solution can detect only the known attacks and the those attacks whose signature is available at the signature database. A new variant DDoS attack is labelled as Economic Denial of Sustainability (EDoS) in cloud environment. This attack is majorly coordinated using the application layer protocols such as HTTP and XML. EDoS protection framework is proposed that involves firewall and puzzle mechanism for detecting the attack [9].

The firewall is enabled for EDoS attack detection at the incoming stage itself and the puzzle server is involved to validate the benign users. The protection framework is implemented in the Amazon Cloud. Since, the method deals with However, it is not conventional firewalls it is not very efficient. Network based intrusion detection system (NIDS) is proposed that brings together Snort and Bayesian method for detecting both known and unknown-attacks in the cloud [10].

The combination of both misuse and anomaly detection is utilized for providing better detection accuracy. Snort acts at the first line of detection for saving the time required for detection. The results illustrate that proposed system yields high detection accuracy with reduced false alarms. Collaborative IDS (CIDS) is proposed that uses Snort for detecting the known attacks that already has their signature in the signature database [11].

Inorder to detect the unknown attacks, there is need for anomaly detection system. The decision tree classifier along with support vector machine (SVM) is used for detecting anomalies. The duration of the learning is reduced because the datasets are divided into multiple subsets. Then SVM is used to learn each subset making the detection fast and efficient. Alerts are correlated and signatures are generated automatically. By doing so, the effects of DDoS attacks are reduced to the greater extent and eventually the performance and detection accuracy of the system in increased. MapReduce based model is proposed for detection of HTTP GET DDoS floods in cloud. Since the MapReduce framework is used it enables fast and accurate detection ensuring the availability of critical system [12]. The proposed system is compared with Snort IDS and the results show that the process time is very less.

III. PROPOSED SYSTEM

The proposed Adaptive Learning based DDoS detection and Automatic Filtering System as depicted in Fig.1. The working method of each module is illustrated in the following section.

A. Adaptive Learning based DDoS Detection

Adaptive learning based DDoS detection is incorporated to detect the variants of DDoS attacks with changing network characteristics. Inspite of the dynamic pattern of the cloud network, the adaptive learning based cloud network intrusion detection system can categorize the DDoS sources and benign sources. It utilizes ruleset to protocol analysis and matching patterns. Based on the rules invoked the IDS can discriminate normal and malicious events. The DDoS sources that are originating from new IP addresses are also detected. It is also capable of identifying various attacks such as port scanning, malformed packet, spoofing, DDoS attacks and still more. The open source network intrusion detection engine SNORT is customized to detect the DDoS attack types.

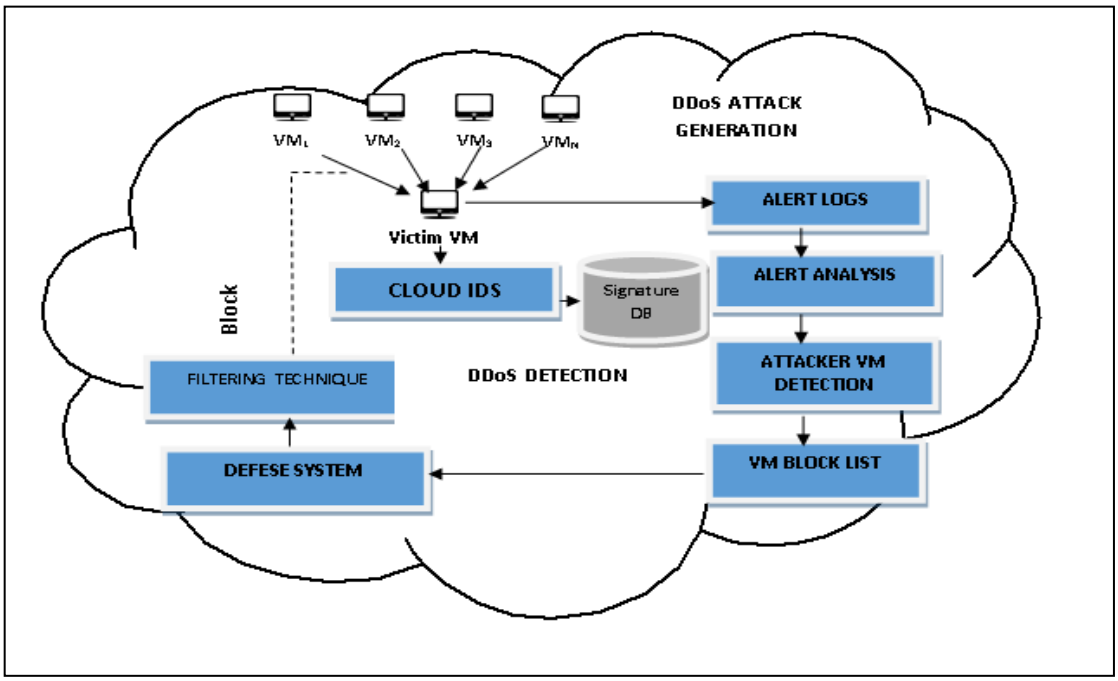

Fig. 1.Proposed System

It detects the known attacks whereas the DDoS variants with different attacking power can go un-noticed. Hence, the rules are customized to detect specific DDoS types such as TCP flood, ICMP flood and UDP flood. The rule-based detection engine is deployed to identify the attackers based on the flow statistics. The flows that match with the ruleset are treated as DDoS attack and alerts are raised per source IP. The threshold based rule detects source IP that crosses the threshold limits. The alerts are logged and directed to the response system for remedial procedures. The basic aspects of snort rules are rule header and rule options. Rule header provides options such as alert, log, pass, activate and dynamic based on which actions can be taken.

Method1:

Solution Ruleset S:=Ø;
Initialize Extended Ruleset E:=Ø;
Insert Custom Rules C_R in the Ruleset E = (C_R,E);
while E ≠Ø do
Select C_R in E;
Match Rules M_R = M□*U M_R: M: Superset M_R = Subset
Generate Alert A_i that contains DDoS Attack IPs D_i;
Append D_i to the Blocklist B;
end while
return S

Fig. 2.DDoS detection using custom method

The rule option provides the alert information once the rules are matched. The cloud IDS is already equipped with inbuilt rules which can detect attacks based on attack pattern matching. The primary objective in selecting the SNORT is that it could be customized to investigate the parameters that needs major attention. DDoS attacks are detected by custom rules and threshold based rules in cloud environment.

The results are compared and contrasted to verify the detection method that is more appropriate interms of detection accuracy, alert reduction and its likelihood in cloud deployment models. The working of the custom method is shown as in Fig.2. The solution set S contains the ruleset that can detect the DDoS attacks. The extended ruleset E contains the custom rules that are written to block the DDoS attack IP sources. The ruleset can be extended to multiple attacks and can detect variants of DDoS attack by appending the new rules to the ruleset E. By doing so, the signature database will be equipped with multiple attack signatures and the cloud IDS is now capable of detecting any kind of attack.

Method2:
Solution Ruleset S:=Ø;
Initialize Extended Ruleset E:=Ø;
Insert Threshold Rules Th_R per flow for (Source, Destination) pair in the Ruleset É = (Th_R,E);
while É ≠Ø do
Select Th_R in É;
Match Rules M_R = M□*U M_R: M: Superset M_R = Subset
Generate Alert A_i that contains DDoS Attack IPs D_i;
Append D_i to the Blocklist B;
end while
return S

Fig. 3.DDoS detection using custom method

The custom rule C_R is selected, and the detection engine checks whether there is a match with attack signature. When the rule is matched with attack pattern the subset M_R is added to the original set M. Followed with, alert A_i is generated by the detection engine which contains the key attributes of the attack source. The attack source IP D_i's are inferred from the alert file and sent to the block list B. The block list B contains the list of DDoS attack sources and it is transferred to the response system for further remedial solution.

The working of the threshold method is shown as in Fig.3. The solution set S is ruleset for detecting DDoS attacks. The extended ruleset E contains the rules to identify the DDoS attack sources. The threshold rule Th_R is selected and the cloud IDS checks matches with attack signature when there is a DDoS attack. Similar to custom method, the subset MR is added to the original set M. Alert A_i is generated for each attack packet and the key elements of the DDoS source is extracted. The attack source IP D_i's are extracted from the alert file and sent to the block list B. The block list B contains the list of sources that are responsible for DDoS flooding attacks and it is passed on to the response system for further action.

The alerts generated by custom method is huge because cloud IDS alerts for each incoming packet. The alerts must be reduced to eliminate the redundancy and processing overhead. For this purpose, the threshold method is incorporated for reducing the alerts in the temporal basis. In the custom scenario, alerts are raised for each packet whenever the ruleset is matched. But in the threshold scenario, the cloud IDS alerts when the attack flow exceeds the threshold defined by the cloud analyst. For example, for every hundred packets, custom method raises hundred alerts whereas threshold method raises only one alert for every hundred packet/second. Hence, threshold method provides the cloud analyst to inspect one alert rather than inspecting hundred alerts thus achieving good alert reduction and speedy processing.

B. DDoS Defense by Automatic Filtering

The proposed system operates on the cloud traffic and system id invoked to find any match with the attack signatures. Based on the matching ruleset, the system can drop, allow or reject the attack sources. The logs are utilized for forensic analysis and inline mode of the IDS is invoked to block the DDoS attack sources. The alerts files are analyzed, and the source IP are extracted for blocking the flooding traffic from the cloud DDoS sources. Attacker VMs are passed to the detection module and passed to the block list file. The defense system blocks the attack traffic and so that legitimate access is not denied as in Fig. 4.

The IPs are obstructed for the given time period and revoked later when the flows are normal in the cloud. DDoS defense is enabled by the automatic filtering of attack traffic so that legitimate sources considerably improve the quality of cloud services and increases the availability. Hence, the packets from the IP address is allowed in the next connection request if they follow non-anomalous behavior. This kind of defense system is dynamic and can adapt with fluctuating attack traffic and various categories of protocol.

Method2:
Solution Ruleset S:=Ø;
Initialize Extended Ruleset E:=Ø;
Insert Threshold Rules Th_R per flow for (Source, Destination) pair in the Ruleset É = (Th_R,E);
while É ≠Ø do
Select Th_R in É;
Match Rules M_R = M□*U M_R: M: Superset M_R = Subset
Generate Alert A_i that contains DDoS Attack IPs D_i;
Append D_i to the Blocklist B;
end while
return S

```
Input : Source_IP
Output : Attack IP
Initialize the number_of_requests
while < limit
   Extract all the IPs based on port using netstat
   Sort the IPs based on port and store in ip_sources
   for all IPs in ip_sources
     do
     if there is a request from IP then increment by 1
     Display "IP with number of connections: n"
   Done
   FLAG=0;
     if n > limit then
     Add a rule in the IP table
     Drop the IP when the request exceeds the limit
     Display " DDoS attack source is blocked
     else
     Display " DDoS attack source is already blocked
   Done
```

private cloud to launch DDoS attack using the experimental set up. Openstack private cloud is used for conducting DDoS experiments. An experimental testbed is built with three private networks and virtual machines to build a DDoS attack topology as in Fig. 5. The two virtual machines from the private network 1 acts as DDoS attacker 1 and DDoS attacker 2 and connects to private network 3 through router 1. One virtual machine from the private network 2 acts as DDoS attacker 3 and connects to private network 3 through router 2. The target virtual machine resides in the private network 3 and connects all the other networks through router 3.

The DDoS attacking scripts are deployed in the attacker machines to execute various flooding attacks such as TCP flood, UDP flood and ICMP flood [13-20]. The cloud DDoS traffic is captured at the victim and investigated for its impact in the cloud. Data is collected and pre-processed before passing to the detection engine [21] and filtered [22].

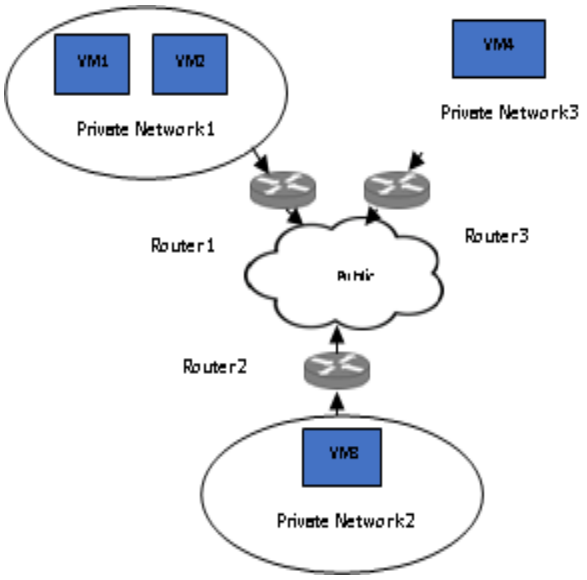

Fig. 5.Experimental Setup

Table- I: Detection Accuracy and Alert Reduction for Various Attacks

Type	Packet Analyzed	Accuracy		No.of Alerts		Alert Reduction
		Custom	Threshold	Custom	Threshold	
ICMP	13477339	99.9	98.05	13476835	11791	99.91
UDP	13186629	99.5	98.07	13126667	10178	99.92
TCP SYN	11318526	77.1	98.53	8727928	5365	99.94

The detection accuracy and alert reduction for custom method and threshold method is compared as in Table I. The detection accuracy for custom method for various attacks such as ICMP, UDP and TCP SYN attack are 99.9%, 99.5% and 77.1%. The accuracy is high when compared to the threshold method where the detection accuracies are 98.05%, 98.07% and 98.52% respectively. The threshold method has 99.91%, 99.92% and 99.94% alert reduction for ICMP, UDP and TCP SYN attack. Hence, the threshold method performs relatively well with 98% detection accuracy for all the attacks and the good alert reduction.

Table- II: Detection Accuracy for ICMP Flood

S.No	Threshold	No.of Alerts	Detection Accuracy (%)
1.	10	1345866	90.01386
2.	100	132850	99.01427
3.	300	43156	99.67979
4.	500	25215	99.81291
5.	700	17545	99.86982
6.	1000	11791	99.91251

Custom method analyses 1347733 packets and provides 13476835 alerts whereas threshold methods generate 11791 alerts achieving 99.91% alert reduction for ICMP flood attack. Custom method analyses 13186629 packets and provides 13126667 alerts whereas threshold methods generate 10178 alerts achieving 99.92% alert reduction for UDP flood attack. Custom method analyses 11318526 packets and provides 8727928 alerts whereas threshold methods generate 5365 alerts achieving 99.94% alert reduction for UDP flood attack.

Number of alerts generated for threshold method for varying threshold limits are as shown in Table II for the ICMP flood attack. For packet sizes 10,100 and 300 the achieved accuracy is about 90.01%, 99.01% and 99.68% and whereas for 500,700 and 1000 the accuracy is about 99.8%, 99.87% and 99.9%. The average detection accuracy for various thresholds are 98.05% for ICMP attack.

Number of alerts generated for threshold method for varying threshold limits are as shown in Table III for the TCP SYN flood attack. For packet sizes 10,100 and 300 the achieved accuracy is about 92.36%, 99.27% and 99.78% and whereas for 500,700 and 1000 the accuracy is about 99.88%, 99.92% and 99.95%.

The average detection accuracy for various thresholds are 98.53% for TCP SYN flood attack. Number of alerts generated for threshold method for varying threshold limits are as shown in Table IV for the UDP flood attack. For packet sizes 10,100 and 300 the achieved accuracy is about 90.06%, 99.03% and 99.69% and whereas for 500,700 and 1000 the accuracy is about 99.82%, 99.88% and 99.92%. The average detection accuracy for various thresholds are 98.07% for TCP SYN flood attack.

Table- III: Detection Accuracy for TCP SYN Flood

S.No	Threshold	No.of Alerts	Detection Accuracy (%)
1.	10	864553	92.36161
2.	100	82638	99.26989
3.	300	25140	99.77789
4.	500	13706	99.87891
5.	700	8884	99.92151
6.	1000	5365	99.9526

Table- IV: Detection Accuracy for UDP Flood

S.No	Threshold	No.of Alerts	Detection Accuracy (%)
1.	10	1310020	90.06554
2.	100	128348	99.02668
3.	300	40832	99.69035
4.	500	23387	99.82265
5.	700	15766	99.88044
6.	1000	10178	99.92282

V. CONCLUSION

The proposed system is validated for its suitability for DDoS attack detection and defense for cloud environment. The custom method and threshold method provide appreciable results in detecting the DDoS attacks in cloud environment with high detection accuracy and good alert reduction. Threshold method provides 98% detection accuracy with 99.91%, 99.92% and 99.94% alert reduction for ICMP, UDP and TCP SYN flood attack. The attack sources are filtered at the victim instance making the applicability of the proposed system in cloud deployment. The future directions in the research is to provide DDoS detection mechanisms based on learning algorithms.

ACKNOWLEDGMENT

This publication is an outcome of the R&D work undertaken project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India, being implemented by Digital India Corporation.

REFERENCES

1. E. Brown, "NIST issues cloud computing guidelines for managing security and privacy," *National Institute of Standards and Technology Special Publication 800-144*, 2012.
2. Top Threats Working Group, "The Notorious Nine Cloud Computing Top Threats in 2013, Cloud Security Alliance", 2013. [Online]. Available:https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf
3. Darren Anstee, "The consequences of DDoS attacks are rising", 2018. [Online].Available:https://www.scmagazineuk.com/consequences-ddos-attacks-rising/article/1490354.
4. Ahmad Nassiri, "5 most famous DDoS attacks", 2018. [Online].Available:https://www.a10networks.com/resources/articles/5-most-famous-ddos-attacks.
5. CSA, "CSA-Guidance/Domain13-Security as a service .md at master", 2017. [Online]. Available:https://github.com/cloudsecurityalliance.
6. S.Potteti and N.Parati, "An innovative intrusion detection system using SNORT for cloud environment", *International Journal of Innovative Research in Computer and Communication Engineering*, vol.3, no.6, June 2015.
7. A.Bakshi and B.Yogesh, "Securing cloud from DDoS attacks using intrusion detection system in virtual machine", *In Second International Conference on Communication Software and Networks*, pp. 260-264, 2010.
8. C.Mazzariello, R. Bifulco and R.Canonoco, "Integrating a network IDS into an Open source Cloud computing", *In Sixth International conference on Information Assurance and Security (IAS)*, pp. 265-270, 2010.
9. S. V. Sandar and S. Shenai, "Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks", *International Journal of Computer Applications*, vol.41, no. 20, pp. 11-16, 2012.
10. K.Patel and R.Srivastava, "Classification of Cloud Data using Bayesian Classification", *International Journal of Science and Research*, vol. 2, no. 6, June 2013.
11. D.Singh, D.Patel, B.Borisaniya and C.Modi, "Collaborative IDS Framework for Cloud", *International Journal of Network Security*, vol.18, no.4, pp.699-709, July 2016.
12. J.Choi, C.Choi, B.Ko, D. Choi, and P. Kim, "Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment", *Journal of Internet Services and Information Security*, vol.3, np. 3/4, pp. 28-37.
13. D.Dittrich, "The DoS projects trinoo distributed denial of service attack tool",1999.[Online].Available:https://staff.washington.edu/dittrich/misc/trinoo.analysis.txt
14. D.Dittrich, "The tribe flood network distributed denial of service attack tool",1999.[Online].Available:https://staff.washington.edu/dittrich/misc/tfn.analysis.txt
15. J.Barlow and W.Thrower, "TFN2K- an analysis, axent security team", 2000.[Online].Available:https://packetstormsecurity.com/distributed/TFN2k_Analysis-1.3.txt
16. D.Dittrich, "The stacheldraht distributed denial of service attack tool", 2016. 2018. [Online]. Available: https://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt
17. D.Dittrich, G.Weaver, S.Dietrich, and N.Long, "The Mstream distributed denial of service attack tool", 2000. [Online]. Available: https://staff.washington.edu/dittrich/misc/ mstream.analysis.txt
18. Bysin. "Knight.c sourcecode", 2001. [Online]. Available: http://packetstormsecurity.nl/distributed/knight.c
19. Rsnake, "Slowloris HTTP DoS", 2016. [Online]. Available https://download.pureftpd.org/misc/slowloris.pl
20. Hping3 network tool, 2019. [Online]. Available: linux.die.net/man/8/hping3
21. SNORT network intrusion detection system, 2019 [Online]. Available: www.snort.org
22. IPtables, 2019. [Online]. Available: linux.die.net/man/8/iptables

AUTHORS PROFILE

B. S. Kiruthika Devi is pursuing PhD at the School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India. Her research interests are cloud security and machine learning. She has completed B.E in Electronics and Communication Engineering in 2002 from Coimbatore Institute of Engineering and Information Technology affiliated to Anna University, Chennai. She has obtained MS (by Research) in Information and Communication Engineering in 2015 from Anna University, Chennai. MS (by Research), work was funded by the National Technical Research Organization (NTRO), New Delhi under Smart and Secure Environment (SSE) project. She has more than six years of experience as a research associate in funded projects from Government of India.

T. Subbulakshmi is currently working as a Professor in the School of Computing Science and Engineering at the Vellore Institute of Technology Chennai. She has good expertise in network security. She has 18 years of teaching experience and she has completed funded projects in the area of security. She has published several research papers in information security and currently guiding five research scholars. Her area of interest includes information security, intrusion detection systems, attack detection and learning algorithms. The author is an expert in developing real time security policies based on open source tools and has publications in 25 journals, 26 international and national conferences, 4 magazines, 4 book chapters and 4 books to her credit.