ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

*Visit: www.ijirset.com*

**Vol. 8, Issue 9, September 2019**

# Taxonomy of Distributed Denial of Service Attacks and Popular Defense Mechanism using Integration of IoT and Cloud Environment

E.Helen Parimala[1], Dr.S.Albert Rabara[2], Y. Sunil Raj[3], A.Vimal Jerald[4]

Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, Tamilnadu, India[1]

Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, Tamilnadu, India[2]

Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, Tamilnadu, India[3]

Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, Tamilnadu, India[4]

**ABSTRACT**: Distributed Denial of Service (DDOS) pose a great challenge to the researchers and other professionals in the domain of data security. Among one of the most serious threats in the area of cloud computing is DDoS. The services to the legitimate users are disrupted by DDoS attacks which are typically explicit attempts. It even leads to shutting down the system and makes the resources unusable through a group of Zombies trying to attack a single target. Moreover, it is hard to trace the actual attacker. Botnets are been setup by attackers to gain access to a huge number of computers by exploiting their vulnerabilities. A coordinated and large scale attack against one or more targets can happen once an attack army has been setup. A desired goal of data of the intrusion detection is to develop a comprehensive defense mechanism against identified and anticipated DDos attack. The immediate need for a detection approach is been highlighted in this work. The main motive behind this work is to show the research community in developing a novel and efficient detection mechanism to address the DDoS problem before and after an actual attack. Intension of this work could help cloud service providers to design more secure cloud environment.

**KEYWORDS**: Distributed Denial of Service (DDOS), Internet of things, Cloud Computing

## I. INTRODUCTION

The forthcoming industrial revolution is in the domain of Internet of Things (IoT) as per various researcher's and expert's opinion [1]. It deals with connecting any devices/products with the Internet using stipulated protocols. This is done for the sake of conducting information exchange and communications for achieving smart recognitions, tracing, positioning and administration. Connecting the network and any service anytime in any place with anything and ideally anyone using some strategies is the main motive of the Internet of Things. The general definition of IoT is the network of physical objects. IoT has evolved into a network of device of all type and sizes and just not only a network of computers. It also includes vehicles, home appliances, smart phones which are all connected, communicated by sharing information with respect to certain predefined standard protocols. This helps in achieving online up gradation, smart reorganizations, process control and administrations [2]. IoT provides users high end scalable infrastructure at an affordable cost. Cloud computing provides on demand internet access and enables ubiquitous computing power which can be provisioned with minimal interaction with its service providers. Near consistent access to their information, data and resources can be done with the help of cloud [3]. Ensuring availability and adaptability of computing resources is done by the Cloud model by reducing the business costs. This is done by simplifying the process of installing software and its associated hardware updates [4].

An agreed level of trust between clients and providers is established through the Cloud computing model. This is very much important to ensure that the organization's novel ideas are secure and also the agreed Quality of Service(QoS) is met [5]. To avoid malicious activity against the provider from insider attacks or security flaws in cloud

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

based applications, a trust from the providers to the clients is established [6]. Due to the advancement in recent technologies, the growth of cloud and internet of things is emerging tremendously. Now a days, a combination of cloud and IoT makes us possible to achieve newer levels of proficiency in conveying administrations, interacting to an enticing business open door for the administrative purposes and to generate revenue. As Information technology grows wider and wider, it makes the cyber attackers to go to a comfort zone of attacking data [7].

Various challenges pertaining to the integration of cloud environment and IoT falls under the category of privacy, security, reliability and Qos [8]. An attractive resource for exploitation from assailants to launch further attacks is in the power of the cloud. For example the biggest DDoS attack in the Norwegian history interrupted online payment systems of five banks, two telecommunication companies, three airlines and one insurance company. It happened all the sudden when a researcher wanted to demonstrate the computing power of the cloud [9]. Among the nine threats to cloud computing environment, DDoS is one among them, according to cloud security Alliance. They have various mechanisms for attacking and large scale distributed infected hosts, making it hard to defend and urgent to be studied[10]. Here, work examines different security parts of Cloud figuring condition, particularly focusing on DDoS. For assailants, there are different free tools accessible on the web and it has turned into a simple assignment for aggressors to complete the assault.

There are different avoidance, discovery, traceback and distinguishing proof strategies to protect the Cloud condition from DDoS assault. Different datasets are additionally accessible for preparing and testing reason, and these datasets are utilized as a benchmark for distinguishing assaults, i.e., in the event that the resistance framework can be effectively tried on these datasets, at that point it can work in any circumstance. Additionally, there are different execution issues, exchange off in putting barrier components and so forth, which must be considered while structuring protection arrangement against DDoS assaults.

The literature overview is being included in next section which has motivated us to carry on with this piece of research. The next section discussed about Architecture of the DDoS attack mechanism. Section 4 of the paper describes Comparisons of various models used to detect DDOS Attack in integration of IoT and cloud. Section 5 shows the Taxonomy of attacks. Finally, the conclusion are discussed.

## II. RELATED WORK

A number of researches had been prepared in DDOS attack detection in cloud that is offered in numerous articles. A small amount of these papers communicated about the DDoS attack is deliberate in this part.

Ayat et al [11] projected a detection system used to discover the DDoS attack in the network through the help of adaptive neuro-fuzzy classifier. The presented method increases the accuracy and reduces the false positive rate. NSL-KDD dataset is used for feature selection. This method produce, accuracy of detection is 96%. Reddy et al [12] have wished-for quantum inspired particle swarm optimization algorithm is used for realize DoS attack in a cloud environment. Decision making technique derived from anomaly detection separated into two sections training and testing. QPSO is used in testing phase to recognize the traffic in the situation arise in attack. This QPSO is compared with superior than QEA Algorithm. Kshirsagar et al [13] have anticipated and implemented system for effective detection of denial of service attack in Local Area Network Environment. The detection mechanism consists of network traffic analyzer, feature extraction. The capable detection of this proposed architecture based on Ip Spoofing. For the duration of the occurrence of memory attack and cpu usage is enlarged and minimized efficiently later than detection of DoS LAND attack. Restriction of this paper the planned mechanism detected only dos attack.

Schiezaro et al [14] have a presented a feature selection method using abc algorithm. The proposed method number of features and also achieve classification accuracy has significantly increased even though the selected number of features has drastically reduced. This method gives better results compared with other methods.

In a Cloud situation, Chonka [15] exhibited calculation to traceback the source by utilizing SOTA. This work indicates how an assailant can start DoS assault on Cloud as HTTP-DoS (HDoS) and XML-DoS (XDoS). The Cloud

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

traceback framework is proposed to discover distinguishing proof of the client and utilizes back proliferation neural system (Cloud Protector) to distinguish and channel the assault messages. It essentially investigations the HDoS and XDoS by utilizing genuine assault traffic and uses SOTA to shield Cloud figuring from these assaults.

The improvement in different resistance instruments, right now rushing to counteract the DDOS assault on the cloud was proposed by [16]. The accepting rate is estimated in MiB/S and the sending rate is in KiB/S as it were. It has demonstrated the directed framework confronted tremendous traffic of SYN flood assaults. On leading the assaults on the private cloud it was discovered that the different equipment and programming firewalls were extremely helpful for diminishing the odds of DOS/DDOS assault. The elements of private cloud and nature of administration are tried and estimated by [17].

In a SYN flood assault, the parcel getting rate is considerably more than the bundle sending rate [18]. Gupta et al. [19] proposed a plan to identify assault example utilizing VM profiling. They have framed the guidelines to recognize the TCP SYN flooding assault by coordinating the dynamic edge qualities granted in parcels. Mishra et al. [20] acquaints a VM checking approach with identify arrange interruption in the cloud. The goal is to perform conduct investigation of system traffic at cloud arrange server (CNS) and cloud figure server (CCoS) and furthermore giving discovery and avoidance of parodying assaults at the virtualization layer of CCoS. The Random Forest methodology gave an exactness of 95.091%. The methodology utilized two degree of security that takes out the requirement for Intrusion Detection System (IDS) on each VM occurrence.

## III. ARCHITECTURE OF THE DDOS ATTACK MECHANISM

One of the genuine assaults that happen in cloud condition is Denial of Service (DOS) assault that makes administration inaccessible for certifiable clients. The administrations to real clients are upset by DDoS assaults which are normally express endeavours. It even prompts closing down the framework and makes the assets unusable through a gathering of Zombies attempting to assault a solitary objective. In addition, it is difficult to follow the genuine assailant. Botnets are been arrangement by assailants to access an immense number of PCs by misusing their vulnerabilities. Botnet attack[21] is said to be an attack that occurs from the group of computers, one will be assigned as the master and the others will be assigned as slaves by the DDoS attack on the victim Computer. During the botnet attack, DDoS tries to interface many systems and they try to contaminate all of them, in that way making the attacker unrevealed. The greatest examples of botnet are said to be MyDoom and Trojan.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

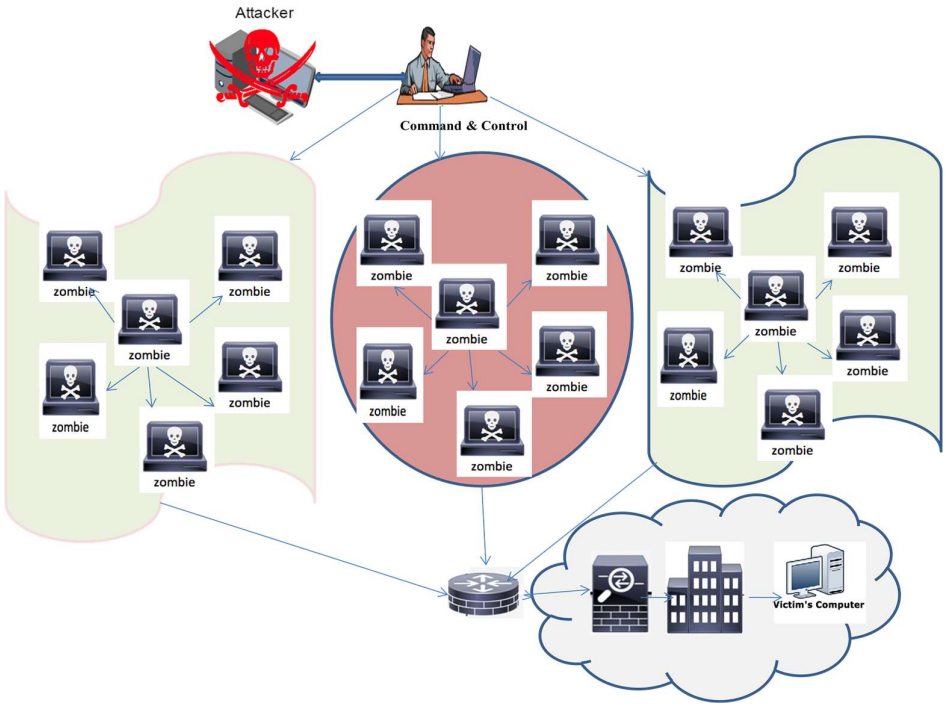


*Fig1. Architecture of the DDoS attack mechanism*

## IV. COMPARISON OF VARIOUS MODELS USED TO DETECT DDOS ATTACK IN INTEGRATION OF IOT AND CLOUD

Mahmod et al [22] have proposed interruption detection using abc optimization algorithm in the midst of neural networks. The abc is used for optimizing the leakage in the weights and bias. NSL-KDD99 dataset is used for feature selection in the course of abc by way of neural networks. The proposed system produce 87.5 % accuracy and it provides 0.124 low error rate. This model used abc in the company of neural networks.

Ali et al [23] have projected artificial neural networks and artificial bee colony bonanza are shared together to enhance the accurateness in detection of DDoS Attacks. This proposed method is used for attribute selection based on weights and thresholds value. Attribute selection can add to the accuracy and speed up the course of DoS detection. The artificial neural networks are a noteworthy procedure to detect new attacks. This method takes a lesser amount of time as compared to other approaches. In this approach, can be able to amplify the efficiency and reduce the error rate and also construct low false alarm rate.

Sharma et al [24] have planned DoS discovery model in cloud via ABC optimization and anomaly based detection performance. This method incorporates two phases training and testing. The training phase incorporates the abc for generating profiles and stored in a database. In the testing phase abc is used for testing the traffic and recovering Dos attacks. The proposed model prove average detection rate of QPSO is 68.3%. Seth [25] have proposed cloud distributed denial of service in the company of artificial bee colony algorithm and also classification and regression tree classifier

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

used for selecting the best feature from the cloud host through CDDOSD proposed algorithm. In this model out of 37 features only 12 features selected for dos attack. They have achieved accuracy in 99% and low false positive rate of 0.0002%.The limitation of this paper is this model only applicable for single threat.

Table 1 DDoS Detection model compared with various methods

| S. No | Author | Proposed Model | Dataset | Accuracy | False Positive Rate |
|---|---|---|---|---|---|
| 1 | Mahmod et al[22] | Network based IDS | NSLKDD99 | 87.5% | 0.124% |
| 2 | Ali et al [23] | Neuro Fuzzy classifier | NSLKDD99 | 96% | 0.002% |
| 3 | Sharma et al [24] | ABC With anamoly detection | Cloud sim | 72.4% | 0.004% |
| 4 | Seth et al [25] | CDDOSD model with ABC | Private Cloud | 99% | 0.002% |
| 5 | Pratheepthi et al [26] | Intelligent rule based system | Cloud sim | 86.4% | 0.008% |
| 6 | Kabir et al [27] | Wrapper Bayesian network approach | NSLKDD99 | 92.4% | 0.004% |

Pradeepthi et al [25] have proposed Wrapper Bayesian network approach for detecting dos attack in cloud using cloudsim tool. They have achieved accuracy for feature selection is 86.4% as well as false positive rate is 0.008%. Kabir et al [27] have presented intelligent rule based system for detecting dos attack in cloud using NSLKDD99 tool. They have achieved efficiency for feature selection is 92.4% and moreover false positive rate is 0.004%.

## V. TAXONOMY OF DDOS ATTACK

There have been a lot of DDoS assaults made by assailants till today and can be delegated pursues. Few of such attacks are discussed and the comparison is tabulated:

### 5. 1.Volume-based attacks

These are most normal sort of DDoS assault. Aggressors attempt to devour the majority of the system transfer speed by sending voluminous number of bundles to an unfortunate casualty server with the goal that it would turn out to be extremely hard for real clients to get to the server because of blockage at interface switches. Greatness of these kinds of assaults is estimated in bits every second. Model: UDP Flood, ICMP Flood, other caricature parcels floods.

### 5.2. Volume-based attacks

These are most typical kind of DDoS strike. Aggressors endeavor to eat up most of the framework move speed by sending voluminous number of groups to a deplorable setback server with the objective that things being what they are to be amazingly hard for genuine customers to get to the server on account of blockage at interface switches. Enormity of these sorts of ambushes is evaluated in bits consistently. Model: UDP Flood, ICMP Flood, other personification bundles floods.

### 5.3. Application layer attacks

The principle rationale of an aggressor is to crash the web server by sending genuine messages or demands to the web server. Size for this assault is estimated as solicitations every second. Model: Slowloris, Zero-day DDoS assault.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

*Table 2: Various types of Denial-of-Service attacks*

| S.NO | Attack Type | Type |
|---|---|---|
| 1 | Back [28] | Application layer attack |
| 2 | RUDY [29] | Application layer attack |
| 3 | Land [30] | Protocol attack |
| 4 | Neptune (SYN Flood) [31] | Protocol attack |
| 5 | Ping of Death (POD) [32] | Protocol attack |
| 6 | Teardrop [33] | Protocol attack |
| 7 | Smurf (ICMP Flood) [34 ] | Volume-based attack |
| 8 | UDP Storm [35] | Volume-based attack |
| 9 | Peer-to-peer [36] | Volume-based attack |

## V. CONCLUSION

This paper, makes a footprint on the study of subtleties of Cloud Security issues and related difficulties. Also have discusses about why DoS and DDoS are significant and potential guarded arrangements in a Cloud domain. Apart from that the work exhibits different execution parameters that are utilized to quantify the exactness and execution of protection frameworks. These can be utilized to analyze various instruments and discover the most ideal arrangement in a given situation. At long last, the work explores different difficulties that are looked by cautious frameworks against DDoS assaults in Cloud environment while detecting, filtering and identifying such attack traffic.

## REFERENCES

[1] Mohammad A.Alsmirat, YaserJararweh, Islam Obidat, Brij B. Gupta, “Internet of Surveillance: A Cloud supported Large Scale Wireless Surveillance Systeml”, the Journal of Supercomputing, Springer, 2016.
[2] Jan Henrik Ziegeldorf1, Oscar Garcia Morchon, and Klaus Wehrle, ”Privacy in the Internet of Things: Threats and Challenges ”, http://dx.doi.org/10.1002/sec.795,2015.
[3] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer “Privacy Expectations and Preferences in an IoT World”, Symposium on Usable Privacy and Security (SCOUPS) 2017, July 12–14, 2017.
[4] Saber Talari, Miadreza Shafie-khah, Pierluigi Siano , Vincenzo Loia , Aurelio Tommasetti , JoaP. S. Catalao ,”A Review of Smart Cities Based on the Internet of Things Concept “,Energies ,2017, doi:10.3390/en10040421.
[5] OvidiuVermesan SINTEF, Peter FriessEU, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems”, river publishers’ series in communications, 2013.
[6] Changbok Jang, Hyokyung Chang, Hyosik Ahn , Yongho Kang “ Profile for Effective Service Management on Mobile Cloud Computing”, DOI: 10.1007/978-3-642-23312-8_17, Advanced Communication and Networking: Third International Conference, ACN 2011, Brno, Czech Republic, August 15-17, 2011. Proceedings (pp.139-145).
[7] M. Waterhouse, “Rutgers University’s computer network under DDoS attack”, http: // abc7ny.com/technology/rutgerscomputer-network-underattack,website-internet-access-down-on campus/1006255, 2015.
[8] S. Sivakumar, V. Anuratha, S. Gunasekaran,” Survey on Integration of Cloud Computing and Internet of Things Using Application Perspective,” International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-6, Issue-4). April 2017.
[9] Xiao, L., Wei, W., Yang, W., Shen, Y., Wu, X., “A protocol-free detection against cloud oriented reflection DoS attacks”, Soft Computing, 21(13), 3713–3721, 2017. doi.org/10.1007/s00500-015-2025-6.
[10] Notorious Nine, “Cloud Computing Top Threats in 2013”, http:// downloads. Cloud securityalliance.org/initiatives /topthreat s/The Notorious Nine Cloud Compuitng Top Threatsin 2013.pdf.
[11] Ayat S, Boroujerdi A.S, “ A robust ensemble of neurofuzzy classifiers DDoS Attack detection”, IEEE International Conference on Computer Science and Network Technology,2013.
[12] Reddy, Pallacali Radha Krishna, Samia Bouzefrane, “ Analysis and Detection of DoS Attacks in Cloud computing by using QSE Algorithm”. High Performance Computing and communications,2014, IEEE.
[13] Deepak Kshirsagar, Amit Rathod, Schin Wathore,“Performance analysis of DoS LAND attack detection,”http://dx.doi.org/10.1016/j.pisc.2016.06.074,2016, elsevier.
[14] Mauricio Schiezaro, Helio Pedrini,” Data feature selection based on artificial bee colony algorithm”,2013, Elsevier.
[15] Chonka, 2010,” Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks”. J Netw Comput Appl 34(4):1097–1107,Elsevier.
[16] Carlin, A., Hammoudeh, M., & Aldabbas, O,2015,”Defence for distributed denial of service attacks in cloud computing”. In Procedia computer science (Vol. 73,pp. 490–497). https://doi.org/10.1016/j.procs.2015.12.037.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

*Visit: www.ijirset.com*

**Vol. 8, Issue 9, September 2019**

[17] Varalakshmi, P., & Selvi, S. T. (2013). Thwarting DDoS attacks in grid using information divergence. Future Generation Computer Systems, 29(1), 429–441. https://doi.org/ 10.1016/j.future.2011.10.012.
[18] Balobaid, A., Alawad, W.,&Aljasim, H, 2016, "A study on the impacts of DoS and DDoS attacks on cloud and mitigation techniques". In International conference on computing, analytics and security trends, CAST 2016 (pp. 416–421). https://doi.org/10.1109/cast.2016.7915005.
[19] Gupta, S., Kumar, P., & Abraham, A, 2013," A profile based network intrusion detection and prevention system for securing cloud environment", International Journal of DistributedSensor Networks. https://doi.org/10.1155/2013/364575.
[20] Mishra, P., Pilli, E. S., Varadharajan, V., & Tupakula, U, 2017, "Out-VM monitoring for malicious network packet detection in cloud". In ISEA Asia security and privacy conference 2017, ISEASP 2017(pp. 1–10). https://doi.org/10.1109/iseasp.2017.7976995.
[21] Deshmukh R. V Devadkar, K. K. (2015),"Understanding DDoS attack and its effect in cloud environment", In Procedia computer science (Vol. 49, pp. 202–210),https: //doi. Org /10.1016 / j.procs. 2015.04.245.
[22] Mahmod, S.M., Alnaish, Z.A.H., Al-Hadi, I.A.A," Hybrid intrusion detection system using artificial bee colony algorithm and multi layer perception", IJCSIS, 2015.
[23] Uzma Ali, Kranti k.Dewangan and Deepak k. Dewangan , " Distributed Denial of Service Attack Dection Using Ant Bee Colony and Artificial Neural Network in Cloud Compuitng",2018, Springer, Advances in intelligent Systems and Computing 652,https://doi.org/10.1007/978-981-10-6747-1_19.
[24] Shalki Sharma, Anshul Gupta, Sanjay Agrawal," An Intrusion Detection System for Detecting Denial of Service attack in Cloud using Artificial Bee Colony",springer,2016, Doi 10.1007/978-981-10-0767-5_16.
[25] Jitendra Kumar Seth, Satish Chandra," An Effective DOS Attack Detection Model in Cloud Using Artificial Bee Colony Optimization", https://doi.org/10.1007/s13319-018-0195- 6,2018,Springer.,2018
[26] Pradeepthi, K. V., & Kannan, A. (2015). Cloud attack detection with intelligent rules. KSII Transactions on Internet and Information Systems, 9(10), 4204–4222. https://doi.org/10.3837/tiis.2015.10.025.
[27] Kabir, M. R., Onik, A. R., & Samad, T. (2017). A network intrusion detection framework based on Bayesian network using wrapper approach. International Journal of ComputerApplications, 166(4), 13–17. https://doi.org/10.5120/ijca2017913992.
[28] Marchette DJ,(2013)," Computer intrusion detection and network monitoring: a statistical viewpoint", Springer Science & Business Media, Berlin.
[29] Enrico C, 2013," Slow DoS attacks: definition and categorization". International Journal Trust Management Computer Communication 1:300–319.
[30] Bujlow T, Carela-Espan˜ol V, Barlet-Ros P,2014," Extended independent comparison of popular deep packet inspection (DPI) Tools for Traffic Classification", http://vbn.aau.dk /files/179043085/TBU_Extended_dpi_report.pdf.
[31] CERT Advisory CA-1996-21, Carnegie Mellon University, 2014, http://www. cert.org/ historical/advisories/ca-1996-21.cfm.
[32] The NSL-KDD Dataset, http://www.unb.ca/research/iscx/dataset/ iscx-NSL-KDD- dataset.html. Accessed 18 Mar 2016.
[33] CERT Advisory CA-1997-28, Carnegie Mellon University, 2014, http://www.cert.org/ historical /advisories/ca-1997-28.cfm.
[34] Lau F, Rubin SH, Smith MH, Trajkovic L ," Distributed denial of service attacks. In: Systems, man, and cybernetics", IEEE international conference on, Nashville, TN, p. 2275–2280 vol. 3, 2000.
[35] Gupta BB, Joshi RC, Misra M, "Distributed denial of service prevention techniques". International Journal of Computer Electronics Engineering.
[36] Badve OP, Gupta BB, " DDoS detection and filtering technique in cloud environment using GARCH model", In: The proceedings of IEEE GCCE-2015, p. 584–586, Osaka, Japan, 2015.