International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

Detecting Application Layer DDoS Attack Based on Rhythm Matrix

Dr.K.Ganesh Kumar[1], T.Advika[2], M.Ishwarya[3], P.V.Kavya Durga[4], M.Keerthiga[5]

Associate Professor, Department of Information Technology, VCET, Erode, Tamil Nadu, India[1]

Student, Department of Information Technology, VCET, Erode, Tamil Nadu, India[2.3.4.5]

ABSTRACT: Application-layer distributed denial of service (AL-DDoS) attacks have become crucial threats to websites as a result of the concealing of AL-DDoS attacks makes several intrusion hindrance systems ineffective. To observe AL-DDoS attacks aimed toward websites, we tend to propose a unique applied math model referred to as the RM (rhythm matrix). though the first options from the network layer square measure adopted, the access flight, together with requested objects and corresponding dwell-time values, may be abstracted associate degreed accumulated into an RM. With an RM, we are able to virtually lossless compress advanced options into a straightforward structure and characterize the user access behavior. we tend to observe AL-DDoS attacks in line with the rise of the abnormality degree within the RM and additional determine malicious hosts supported change-rate outliers. within the experiments, we tend to simulate 3 modes of AL-DDoS attack switch the latest popular DDoS attack tools: LOIC and HOIC. The results show that our technique will observe these simulated attacks and determine the malicious hosts accurately and expeditiously. For associate degree AL-DDoS detection technique, the power to differentiate flash crowds is indispensable. we tend to additionally demonstrate the wonderful performance of our approach in characteristic flash crowds from AL-DDoS attacks with two reconstructed public data-sets

KEYWORDS: DDoS Attack, Rhythm Matrix, Malicious Host, Denial of service, Security.

I. INTRODUCTION

Application layer DDoS attacks became terribly effective within the world of cyber attackers. They basically represent a sophisticated quite DDoS attack, quite sort of a Special Forces analogy, in this they're terribly laborious to sight, they often appear initiate legitimate and they're focus is generally not on volume, however on little extremely skillful or extremely advanced DDoS attack sequences. nonetheless, even if application layer DDoS attacks area unit little and non-cliometrics they're as effective as the other volume-based DDoS attack basically rendering your business down, otherwise discontinuous. Application layer DDoS attacks area unit DDoS attacks on layers five through seven within the OSI stack each across the board like: FTP, SMTP, HTTP, HTTPs, TLS also as some business crucial VoIP applications or extremely something that your organization can be exploitation. For DDoS protection against application layer DDoS attacks, you're reaching to have to be compelled to have a sophisticated, terribly shut application sight ion technology that may not solely be able to detect robustly a activity component of a legitimate association, however are able to move that DDoS mitigation in to the cloud to take it off from your applications as quick as attainable. The activity component has been driven as a result of basically of the character of application layer DDoS attacks.

In order to defend against AL-DDoS attacks effectively, we have a tendency to propose RM (rhythm matrix) that extracted rhythm patterns to represent the characteristics of music clips.Once the packet size and also the entomb point in time of consecutive HTTP-request packets in an exceedingly flow as our original options. when a series of transformation, the relative relations area unit extracted from feature sequences to construct the RM (rhythm matrix). For web site users, the RM will characterize the distribution of their access mechanical phenomenon fragments, as well as the order of visiting pages and also the time spent on every page. it's tough for AN assaulter to mimic these characteristics of legitimate access. So, we have a tendency to examine the change-rate abnormality within the RM to sight AL-DDoS attacks, and additional determine the malicious hosts in step with their drop points within the RM. Our methodology provides a brand-new perspective for each characterizing cluster behaviors and characteristic AL-DDoS attacks. Analysis and experiments show that our methodology performs well in terms of each timeliness and accuracy.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

II. RELATED WORK

The application layer distributed denial of carrier (DDoS) attacks have come to be an extreme hazard to the protection of net servers. These attacks sidestep most intrusion prevention structures via sending several benign HTTP requests. Since most of these assaults are launched unexpectedly and severely, a quick intrusion prevention machine is perfect to notice and mitigate these assaults as quickly as possible..[26]The detection of DDoS attack carried out with the help of the network capacity (called as router capacity) in processing and forwarding of the information packets.The packet flow is analyzed with the help of Z-Test to check whether there is an abnormal traffic occurred in the network by focusing on the data arrival rate at different time interval.Based on the result,the information packets are analyzed and check with the threshold value for forwarding processing by the router.

III. METHODOLOGY

Generally, the word ‘‘rhythm’’ is used to refer to all the temporal components of a musical work. In the field of music sign processing, rhythm has been extracted as a characteristic for detecting tune temper or classifying the style of the music content. Based on the rhythmic characteristics of network flow, we recommend RM and use it to discover AL-DDoS attacks. A Rhythm matrix is used to symbolize the styles of site visitors in DDoS detection. This technique constructed a behavior feature matrix based on nine consumer behavior capabilities, and outliers from person surfing behavior patterns had been used to recognize normal users and attackers. Compared with the get right of entry to matrix, our rhythm matrix also can seize the spatial-temporal styles of get entry to behaviors with decrease complexity. The rhythm matrix is constructed on the packet level, as is the visitor’s matrix, but the features employed by means of the rhythm matrix can depict a mile’s richer application-layer information.

Construction of RM (rhythm matrix)

Rhythm Matrix Let F be the packet sequence of a traffic trace, the transformed sequence of that's F0. The RM is a 10d × 10d lattice, with Rxy indicating the component at area (x, y) of the network. If the fee of every element Rxy is same to the frequency of (x, y) in F0, it is named that RM the rhythm matrix of this trace.It described by the pair of (x, y) which is calculated by the frequency of (x, y) during one window and the row and column of the 10 x 10 matrix is used to calculate the frequency and analysis the traffic involved in the server of the RM is constant, so the time complexity is O (1). When it discovers malicious hosts, we first perform outlier detection.

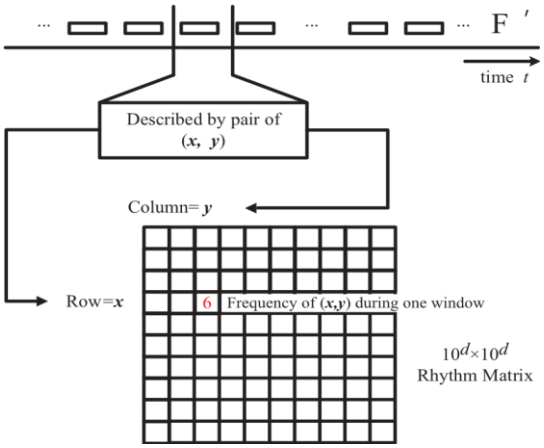

Figure 1. Rhythm matrix construction

This did not set the window on F but on F^0, and the dimensions of the window is primarily based at the quantity of drop points. On the hand, a time-based window on F might lead to more computational overhead inside the absence of

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

DDoS assaults and rare access. Then again, a window size dependent on the quantity of bundles would produce different RMs on account of glimmer swarm traffic.

Data transformation

The encapsulation headers always preserve a hard and fast period for a client-server pair, and the payload is the main variable for one-of-a-kind utility protocols. For HTTP requests, the scale of payload is the sum of the lengths of the URL and HTTP protocol extra messages. For a given website, the best version is the extra messages, which rely on some factors with a small variable quantity. Thus, the packet length s corresponds to the period of the URL. The inter arrival time between consecutive packets is stricken by many factors, such as the space of the peers, community congestion, and user get entry to behavior. We undertake a logarithmic transformation to truncate the range of possible values to a restricted interval. Commonly, the grain of the time-stamp recorded by using a community traffic capture device is fixed. Hence, the determined variable log10[Δt] is discrete and limited.

Malicious host identification

The comparable access behavior of a tremendous variety of malicious hosts results in abnormal boom elements, and vice versa, the bulk drop points of one malicious host would fall on abnormal increase elements. Thus, if the abnormal increase elements are determined out, we will discover the malicious hosts. By considering the change-rate outliers, we will discover the abnormal growth elements in RM. In statistics, an outlier is a statement point that is distant from different observations. The simplest manner to become aware of outliers is with the quartile method, which flags observations based totally at the interquartile variety.

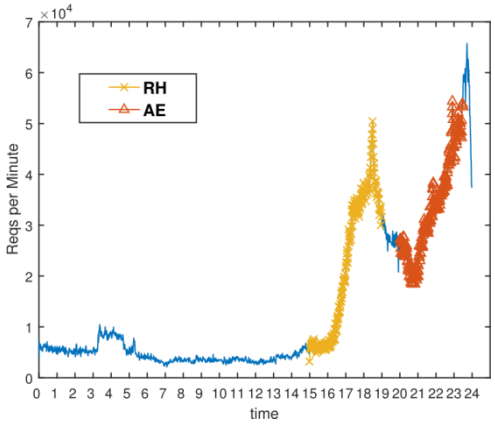

Figure 2. Flash crowd dataset

Complexity analysis

The computational complexity of the technology of an RM is O(n), wherein n is the quantity of drop factors inside the RM and is no more than PktW. A hash desk is used to record the list of packet lengths and inter arrival times (s, Δt), that's reallocated and does no longer increase, so the spatial complexity is O (1). To generate the abnormality degree of every RM in the detecting phase, we need to calculate the change-prices and count them. The number of elements in the time complexity to come across outliers is related to the sorting algorithm: we use quick-sort with time complexity O (n ∗ log2n). After an attack is detected, we track every IP and calculate the percent of drop factors falling on outliers Application layer-DDoS attacks target the web-sites and consider HTTP-flood attacks as the principal. The main objective is to build an accurate rate of the traffic analysis. It tries to detect whether the traffic is degraded with the flow of attacks by comparing the behavior with the target class

Performance of detecting AL-DDoS attack

The predominant statistics samples have been generated with the aid of a small-scale simulation. This evaluate the effectiveness and timeliness of the proposed method. The statistics have been amassed via mirroring the server's Ethernet port and taking pictures the inbound traffic. Our AL-DDoS detecting approach is primarily based on two assumptions, one is that the RMs of site visitors centered at the equal internet site are similar, and the different is that AL-DDoS attacks would motive apparent modifications in the RMs. We set Pktw to be 2000 and chosen two RMs at irregular from ordinary traffic, LOIC-S, HOIC-P and HOIC-P, individually. The 2000 drop factors are in moderation allotted in 1000*1000 matrix, which is hard to be located by way of the unaided eye. So, we compacted these 102 × 102 matrices into 50 × 50 matrices through amassing adjoining elements As should be obvious, the varieties between RMs from standard traffic, LOIC-S, HOIC-P and HOIC-P are self-evident, and the frameworks in the *equivalent group* are fundamentally the same as.These statistical outcomes strongly help our assumptions. To consider our detection method, we calculate the actual high-quality fee (TPR) and false high-quality fee (FPR*)*.A large Pktw should lengthen the detection time, however a small window dimension should additionally weaken the statistical traits of the rhythm matrix. Taking these elements and the dataset dimension into account, we set Pktw in the vary 800˜2200 with step 200. Before attack detection, the threshold abnormality degree, must be set. The packets which carries empty TCP will not be considered, except for those which SYN/FIN TCP flags are set. Incoming packets must be filtered out from F. The behavior packets of zero payload size does not depend on the behavior of the user but it is a function of the TCP/IP stack of the end host and status of the network which reduce the consumption of the computational resources.

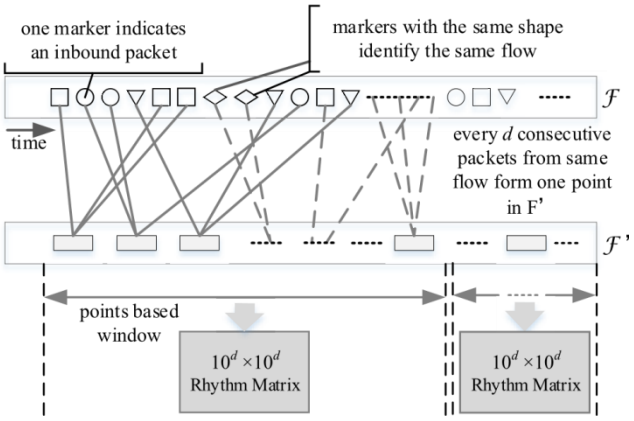

Figure 3.10 x 10 Rhythm Matrix

Comparison with another DDoS host

This section shows the comparison of our proposed system with the existing system in terms of four key aspects: complexity, accuracy, adaptation and data source.From the regular and one type of DDoS traffic, we collect P and Q RMs respectively, which denoted via Norm and RM DDoS. Then, we carry out detection and calculate the TPR and FPR.For three kinds of AL-DDoS attacks, our approach carried out properly in phrases of each TPR and FPR.The entropy of the user's HTTP request sequence geared up to the model is used as a criterion to measure the user's normality. This approach ought to attain an FPR as low as 1.5% and a detection price of about 90%.Based on the analysis of the traffic of the DDoS attack, efficient method called rhythm matrix for the DDoS detection in a network, the technique on the in the past referred to actual flash crowd dataset and checked the abnormality degree.This dataset consists of some normal visitors and two flash-crowd periods, i.e., RC and AE; therefore, we surely replayed the visitor's facts to the detection system. We selected a Pktw of 1400, and set the threshold zero = 590 primarily based on a length of normal traffic. The abnormality levels of flash crowd site visitors have been dispensed in the equal vary as regular site visitors and did no longer exceed the threshold. Therefore, an everyday unexpected visitors spike, i.e., a flash crowd, ought to now not be incorrect for an AL-DDoS attacks

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

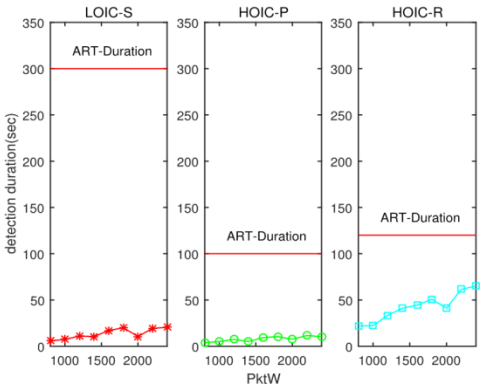

Figure 4.Timeline of DDoS attack Detection

Table 1.Performance of identified malicious host

Θ	Precision			Recall		
	LOIC-S	HOIC-P	HOIC-R	LOIC-S	HOIC-P	HOIC-R
0.2	1.00	1.00	0.69	1.00	1.00	1.00
0.4	1.00	1.00	0.92	1.00	1.00	1.00
0.6	1.00	1.00	1.00	1.00	1.00	1.00
0.8	1.00	1.00	1.00	1.00	0.82	0.27

IV. EXPERIMENTAL RESULTS

DDoS attacks on application layer

A wide range of DDoS attacks goal the community bandwidth due to the fact of the ease with which it can be exhausted. Attackers absolutely ship a giant quantity of community packets to the server, efficaciously arduous the community bandwidth. Network layer protocols like UDP (User Data gram Protocol) and ICMP (Internet Control Message Protocol) are used for this purpose. As time passed, two matters changed. Networks and servers grew to become greater sturdy in figuring out community layer DDoS assaults and servers should find the money for higher and accelerated bandwidth. A particularly massive quantity of requests should nonetheless exhaust the community bandwidth and take down a server, however it grew to become extra tough to do so. The attackers answered by using transferring up the stack to the transport layer. SSL renegotiation at exploited attacks in the transport layer, however as time surpassed servers started out to shield in opposition to these attacks as well. These attacks had a sample that should be recognized and generalized throughout platforms, and ought to be strictly categorized as malicious.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

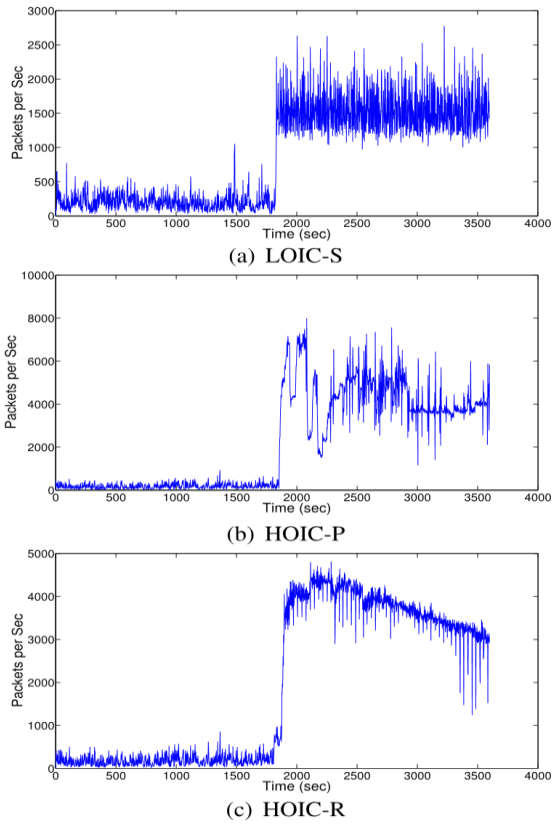

Figure 5. Three different DDoS attack

In latest years, attackers have moved up the stack one extra time giving upward jostle to a new fashion known as utility layer DDoS attacks. These attacks have no longer intention to throttle the community bandwidth, alternatively they strive to exhaust server sources like CPU cycles, database cycles, reminiscence or socket connections. There has been a massive increase in the quantity of software layer DDoS attacks in the current years. Imperva Incapsula's Global DDoS Threat Landscape Report 2017 reviews that for the fourth quarter in a row, there used to be a minimize in the quantity of community layer assaults alongside with any other spike in the range of software layer assaults. Reports by way of Kaspersky point out the reality that "the cream of cybercriminal communitiesare now turning to Application Layer DDoS attacks". Attacks carried out at the software layer have a few subtleties which makevaluable traffic to the website, and it would be detrimental to the website if they were wrongly labelled as DDoS traffic and them special and exclusive from different attacks.

- *Legitimate requests*: Application layer DDoS assaults proceed thru respectable HTTP packets. There is surely no distinction between an assault request and an ordinary request. The solely distinction resides in intent, and no longer in content. This makes most community stage packet filters and even some software layer firewalls ineffective in detecting these attacks.
- *Low Traffic Volume*: Contrary to community layer DDoS attacks, the place the community bandwidth will become the bottleneck, in software layer DDoS attacks, the server assets emerge as the bottleneck. Because of that, the server can be delivered down the usage of comparatively fewer requests, and subsequently the visitor's extent is additionally low. Most of the current DDoS detection mechanisms count on the massive visitor's quantity to perceive attack. That method fails in the case of software layer DDoS attack, making most of the present DDoS detection mechanisms obsolete.

***Datasets*:** The scan data sets utilized by way of prior pupils had been mixed, whilst some relied solely on one dataset. The utilization of exclusively one dataset as reference (e.g., benchmark and investigation) seems lacking as HTTP DDoS assault designs are shifted. Further evaluation carried out took into account greater than one dataset.

Table 4. Performance of detecting DDoS attack

PktW	*TPR*			*FPR*		
	LOIC-S	HOIC-P	HOIC-R	LOIC-S	HOIC-P	HOIC-R
800	1.00	1.00	1.00	0.00	0.00	0.01
1000	1.00	1.00	1.00	0.00	0.01	0.00
1200	0.99	0.99	1.00	0.00	0.01	0.01
1400	1.00	1.00	1.00	0.01	0.00	0.00
1600	0.99	1.00	1.00	0.00	0.00	0.00
1800	0.99	1.00	0.99	0.00	0.00	0.00
2000	0.99	0.99	1.00	0.00	0.00	0.00
2200	1.00	1.00	1.00	0.00	0.00	0.00

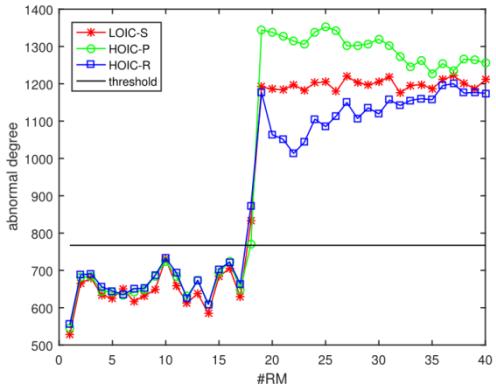

Figure 6.Abnormity degree and edge for various sorts of traffic.

Nevertheless, the used datasets have been out of date to function assessment and analysis. Critical inspection in opposition to researchers who employed extra than one dataset confirmed that they additionally accomplished their experiments to achieve the dataset. Old datasets have to be averted as they incorporate out of date and meaningless facts [9], while retrieving actual latest attack dataset is difficult as they are unavailable public. As appeared in Table 2, for three kinds of AL-DDoS assaults, our strategy performed well as far as both TPR and FPR.

V. CONCLUSION AND FUTURE SCOPE

This paper proposed a new model, i.e., the rhythm matrix, to represent access behaviour. Based on this model, the odd change factors of the RM are utilized to observe AL-DDoS attacks and to pick out malicious hosts. We simulated three modes of DDoS attacks through the use of the state-of-thread AL-DDoS attack equipment LOIC and HOIC on our campus network. The contrast verified that our strategy performs nicely in phrases of each accuracy and timeliness. At remaining count, the TPR is over 99% and the FPR is no greater than 1%. The precision and recall of figuring out malicious hosts multiplied to almost one hundred percent with the optimization of the parameters. All the simulation attacks had been detected a way until now than the time at which they took effect. Furthermore, two datasets modified from the 1998 FIFA World Cup dataset illustrated that our approach possesses terrific overall performance in the situation of flash crowds. In our model, though the site visitors elevated drastically beneath flash crowds, the abnormality diploma did no longer increase, whereas the abnormality diploma did amplify below AL-DDoS attack.We have tried to minimize the complexity of AL-DDoS detection approach and proposed the rhythm matrix as a model with robust identification power. Our future work will combine the rhythm matrix with different on-line detection methods.

A few boundaries are well worth discussing. First, the overall performance of our technique may additionally be influenced with the aid of community conditions. Our approach was once designed to run on a side router close to the net server. If the technique is deployed on a spine router, it must be successful of coping with the excessive bandwidth by way of putting a large PktW, however the detection time would be barely delayed. Second, state-of-the-art attackers may also amplify AL-DDoS site visitors slowly, and our approach may additionally now not be capable to observe the change. To overcome this vulnerability, we can pick out greater than one base matrix over a longer horizon, accordingly the abnormality diploma ought to be amassed sufficiently to observe the slowly growing attack. Furthermore, low price DoS attack towards functions (LoRDAS) may additionally reason issues due to the fact the exclusive attributes of LoRDAS stop our method from detecting such attacks all through the manifestation phase, until the attacker is enough to disturb the rhythm matrix. Finally, two thresholds, i.e., zero and Θ, have to be set primarily based on historic facts of thegoal website. Alternatively, we should undertake a cluster algorithm to differentiate odd data. The clustering scheme should keep away from the trouble of placing experimental values however would end result in greater computational complexity. In practice, we want a stability between complexity and convenience.

ACKNOWLEDEMENTS

We express our deepest sense of gratitude towards our respected and noble guide Dr.K.Ganesh Kumar Sir for spending hisvaluable time on several occasions to impart us the gains of his knowledge. It was our privilege to have worked under hisguidance. we shall always remain indebted to him. We wish to express our earnest thanks to the Industrial adepts for providing us the opportunity to explore the feasible options that were available to us.

REFERENCES

[1]. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, ‘‘Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods,’’ IEEE Access, vol. 7, pp. 51691–51713, 2019.
[2]. Bhardwaj and S. Goundar, ‘‘Comparing single tier and three tier infrastructure designs against DDoS attacks,’’ International. Journal. Cloud Application. Computer., vol. 7, no. 3, pp. 59–75, Jul. 2017.
[3]. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Li, and L. Gong, ‘‘Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN,’’ *Int. J. Commun. Syst.*, no. 2, no. 5, 2018, Art. no. e3497.
[4]. B. Rawat and S. R. Reddy, ‘‘Software defined networking architecture, security and energy efficiency: A survey,’’ *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 325–346, 1st Quart., 2017.
[5]. H. Peng, Z. Sun, X. Zhao, S. Tan, and Z. Sun, ‘‘A detection method for anomaly flow in software defined network,’’ *IEEE Access*, vol. 6, pp. 27809–27817, 2018.
[6]. J. David and C. Thomas, ‘‘Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic,’’ Computer. Security., vol. 82, pp. 284–295, May 2019.
[7]. J. Faigl and G. A. Hollinger, ‘‘Autonomous data collection using a selforganizing map,’’ *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 5, pp. 1703–1715, May 2018.
[8]. J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, ‘‘A DDoS attack detection method based on SVM in software defined network,’’ *Secur. Commun. Netw.*, vol. 2018, Apr. 2018, Art. no. 9804061.
[9]. K. Kalkan, G. Gür, and F. Alagöz, ‘‘Filtering-based defense mechanisms against DDoS attacks: A survey,’’ IEEE System. J., vol. 11, no. 4, pp. 2761–2773, Dec. 2017.
[10]. K. S. Sahoo, S. K. Panda, S. Sahoo, B. Sahoo, and R. Dash, ‘‘Toward secure software-defined networks against distributed denial of service attack,’’ *J. Super comput.*, vol. 75, no. 8, pp. 4829–4874, 2019.
[11]. L. Zhu, X. Tang, M. Shen, X. Du, and M. Guizani, ‘‘Privacy-preserving DDoS attack detection using cross-domain traffic in software defined networks,’’ *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 628–643, Mar. 2018.
[12]. M. E. Ahmed, S. Ullah, and H. Kim, ‘‘Statistical application fingerprinting for DDoS attack mitigation,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 6, pp. 1471–1484, Jun. 2019.
[13]. M. Ge, J. B. Hong, S. E. Yusuf, and S. K. Dong, ‘‘Proactive defense mechanisms for the software-defined Internet of Things with nonpatchable vulnerabilities,’’ *Future Generat. Comput. Syst.*, vol. 78, no. 2, pp. 568–582, Jan. 2018.
[14]. M. Kamarudin, C. Maple, and T. Watson, ‘‘Hybrid feature selection technique for intrusion detection system,’’ International. Journal. High Perform. Computer. Network., vol. 13, no. 2, pp. 232–240, 2019.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

[15]. M. Latah and L. Toker, ''Towards an efficient anomaly-based intrusion detection for software-defined networks,'' *IET Netw.*, vol. 7, no. 6, pp. 453–459, Nov. 2018.

[16]. M. R. Haque, S. C. Tan, Z. Yusoff, C. K. Lee, and R. Kaspin, ''DDoS attack monitoring using smart controller placement in software defined networking architecture,'' in *Computational Science and Technology*. Singapore: Springer, 2019, pp. 195–203.

[17]. O. Rahman, M. A. G. Quraishi, and C.-H. Lung, ''DDoS attacks detection and mitigation in SDN using machine learning,'' in *Proc. IEEE World Congr. Services (SERVICES)*, Jul. 2019, pp. 184–189.

[18]. R. Swami, M. Dave, and V. Ranga, ''Software-defined networking-based DDoS defense mechanisms,'' *ACM Computer. Survev.*, vol. 52, no. 2, 2019, Art. no. 28.

[19]. S. Dong, K. Abbas, and R. Jain, ''A survey on distributed denial of service (DDoS)attacks in SDN and cloud computing environments, '*IEEEAccess*, vol. 7, pp. 80813–80828, 2019.

[20]. S. Dong, K. Abbas, and R. Jain, ''A survey on distributed denial of service (DDoS)attacks in SDN and cloud computing environments, 'IEEEAccess, vol. 7, pp. 80813–80828, 2019.

[21]. S. Hosseini and M. Azizi, ''The hybrid technique for DDoS detection with supervised learning algorithms,'' Computer. Network., vol. 158, pp. 35–45, Jul. 2019.

[22]. T. H. Nguyen and M. Yoo, ''A hybrid prevention method for eavesdropping attack by link spoofing in software-defined Internet of Things controllers,'' *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 11, pp. 1–9, Nov. 2017.

[23]. T. M. Nam, P. H. Phong, T. D. Khoa, T. T. Huong, P. N. Nam, N. H. Thanh, L. X. Thang, P. A. Tuan, L. Q. Dung, and V. D. Loi, ''Self-organizing mapbased approaches in DDoS flooding detection using SDN,'' in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2018, pp. 249–254.

[24]. T. V. Phan, N. K. Bao, and M. Park, ''Distributed-SOM: A novel performance bottleneck handler for large-sized software-defined networks under flooding attacks,'' *J. Netw. Comput. Appl.*, vol. 91, pp. 14–25, Aug. 2017

[25]. T. Wang and H. Chen, ''SGuard: A lightweight SDN safe-guard architecture for DoS attacks,'' *China Commun.*, vol. 14, no. 6, pp. 113–125, 2017.

[26]. K.Ganesh kumar and N.Rangarajen, "Detection of DDoS attack by monitoring network traffic by using Z-Test based Satistical Analysis,"Asian Journal of Information Technology.,15(24):5193-5196,2016.