ISSN:0975-9646
Sathish Kumar S et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 13 (3) , 2022, 68-75

Forestalling Denial of Service Attack in Cloud Computing and Predicting Future Attack using Machine Learning

Sathish Kumar S, Sarath Kumar S, Vignesh VS*, Mrs. R. Thillaikarasi**
*(Department of CSE, Kingston Engineering College, Vellore
Email: sathish04virgo@gmail.com)
** (Department of CSE, Kingston Engineering College, Vellore
Email: balajicse.engineering@kingston.ac.in)

***Abstract*— In our task a complex system to coordinate secretive assault designs against applications running in the cloud. Rather than targeting making the assistance inaccessible, the proposed system targets taking advantage of the cloud adaptability, driving the application to consume a larger number of assets than required, influencing the cloud client more on monetary perspectives than on the help accessibility. The assault design is coordinated to avoid, or be that as it may, enormously postpone the procedures proposed in the writing to recognize low-rate assaults. It doesn't display an occasional waveform regular of low-rate depleting assaults. Conversely, with them, it is an iterative and steady interaction. Specifically, the assault strength (as far as administration demands rate and simultaneous assault sources) is gradually improved by a patient aggressor, to cause critical monetary misfortunes, regardless of whether the assault design is acted in understanding to the greatest work size and appearance pace of the help demands permitted in the framework. Utilizing an improved-on model exactly planned, we determine an articulation for slowly expanding the power of the assault, as a component of the arrived at administration corruption (without knowing ahead of time the objective framework capacity). We show that the highlights presented by the cloud supplier, to guarantee the SLA haggled with the client (counting the heap adjusting and auto-scaling components), can be vindictively taken advantage of by the proposed secretive assault, which gradually debilitates the assets given by the cloud supplier, and expands the costs brought about by the client.** (1)

***Keywords*— DDoS attack, multiple linear regression, tra*ffi*c packet, classification, SIPDDOS, SDN**

I. INTRODUCTION

All things considered; Denial of Service (DoS)attacks are expected essentially to disturb registering frameworks in an organization. Essentially, these assaults are started from a solitary machine with the ill-conceived intension of focusing on a server framework through an assault. A straightforward DoS assault could be a PING Flood assault in which the machine sends ICMP solicitations to the objective server and an additional mind-boggling DoS assault model could be Ping of death assault. DDoS (Distributed Denial of Service) assaults are postcursor tasks assaults, i.e., DoS assaults are herald to DDoS assaults. DDoS assaults are the assaults which are conveyed in dispersed conditions. In a general sense, a DDoS assault is a deliberate assault type which is typically made in a circulated registering climate by focusing on a site or a server to limit their typical exhibition. To accomplish this, an assailant involves various frameworks in an organization. Presently, utilizing these frameworks, the aggressor makes an assault on the objective site or server by making different solicitations to the objective framework or server. As these kinds of assaults are completed in disseminated conditions, thus, these are likewise called circulated DDoS assaults.

The customary method of DDoS assaults is the animal power assault that is set off utilizing Botnet wherein the gadgets of the organization climate are contaminated with malware. In view of the objective and the way of behaving, we might group DDoS assaults into three classes. In this way, however DDoS assaults could be
ordered into a few kinds, generally these assaults are fundamentally grouped into three classes. They are
Traffic/discontinuity assault, (ii) Bandwidth/Volume assault and (iii) Application assault as displayed in Figure1. In tra ffic-based assaults, voluminous UDP or TCP bundles are shipped off the objective framework by the assailant and these immense UDP or TCP parcels diminish the framework execution. In the second kind of assault called transmission capacity or volumetric assaults, the aggressor makes blockage in transfer speed through consuming over the top data transfer capacity than required genuinely and they additionally attempt to flood the objective framework through sending a lot of unknown information. The last kind of assault are likewise particular assaults as they are pointed toward going after just a particular framework or an organization. These sorts of

assaults are likewise hard to relieve and toss more prominent difficulties in remembering them.

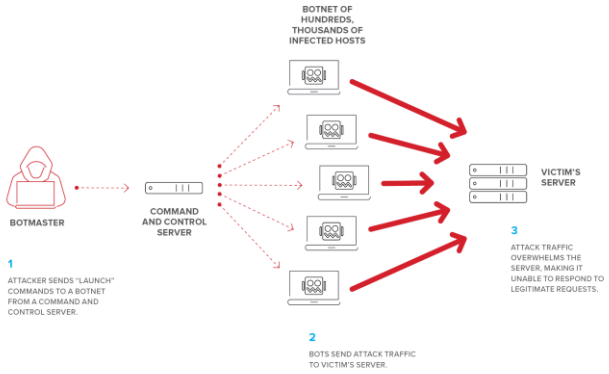

Fig1: Concept of DDOS ATTACK

As a rule, a Denial of Service assault, which is generally called a DoS assault, is an intentional Endeavor which is started to make an application or site inaccessible to its genuine clients. This is accomplished as a rule by flooding the site or application through network traffic. To accomplish this, normally, one of the few selections of aggressors is to apply broadened strategies that purposefully consume immense organization transfer speed, subsequently making burden real clients. Then again, aggressors likewise accomplish this by dealing with framework assets in an ill-conceived way. DoS assault is additionally called Non-circulated Directed assault wherein an assailant starts DoS assault on the objective framework. The idea of DDoS assault is like DoS assault however the key distinction is that in DDoS assaults there are numerous assault sources which are certainly involved, i.e., in DDoS assaults, the aggressor makes an assault by utilizing different sources which might incorporate switches, IoT gadgets, and PCs in a conveyed climate tainted by malware. To make this conceivable, an assailant searches for accessibility of any compromised network. By using such compromised networks, an aggressor for the most part goes after the objective framework through persistently creating bundle floods or demands to overcome the objective framework. The DDoS assaults are normal in the Network layer, Transport layer, Presentation and Application layer of the 7-layer OSI reference model. Network layer and Transport layer assaults are generally called Infrastructural assaults while the Presentation layer and Application layer assaults are normally known as Application layer assaults.

II. RELATED WORK

S.Shanmuga Priya; M.Sivaram; D.Yuvaraj; A.Jayanthiladevi (2020) proposed “Machine Learning based DDOS Detection”,One of a high constant assault is the vital conveyed DoS attacks. The sorts and devices for this attacks increments everyday according to the innovation increments. So the philosophy for recognition of DDoS ought to be progressed. For this reason we made a computerized DDoS identifier utilizing ML which can run on any ware equipment. The outcomesare 98.5 % precise. We utilize three order calculations KNN, RF and NB to characterize DDoS parcels from typical bundles utilizing two elements, delta time and parcel size. This finder generally can recognize a wide range of DDoS like ICMP flood, TCP flood, UDP flood and so on. In the more established frameworks they distinguish just a few kinds of DDoS assaults and a few frameworks may require countless elements to distinguish DDoS. Some frameworks might work just with specific conventions as it were. Be that as it may, our proposed model defeat these disadvantages by identifying the DDoS of any kind without a need of explicit convention that purposes less measure of elements.

Subhashini Peneti, Hemalatha E (2021) proposed “DDOS Attack Identification using Machine Learning Techniques”,One of the serious issues that the world faces today is digital assaults. Forswearing of Service assaults have been one of mostincessant assaults. A portion of the moderating procedures are whitelisting/boycotting IP addresses, rate restricting and so on. The significant objective of any DoS assault is to cut down the standing of the casualty association. In this way, rather than confronting
the issues after the assault, fostering a savvy identification system is generally prudent to recognize and forestall DoS assaults. While there are numerous approaches to recognize DoS assaults, applying AI strategies to recognize and forestall the assaults ends up being a promising one. Since there is a great deal of information accessible about DoS assaults, machine learning calculations can identify examples of these DoS assaults and accordingly apply these examples to new asks for and characterize them as pernicious or harmless requests.We think about the CICIDS2017 dataset. The dataset has information connected with solicitations of 7 days of a week. Among those, Wednesday's dataset contains records connected with kinds of DoS assaults. Despite the fact that methods like AdaBoost, XGBoost and brain organizations can be applied, arbitrary timberland gives incredible execution.

Anupama Mishra, B. B. Gupta, Dragan Perakovi´c, Francisco Jos´e Garc´ıa Pe˜nalvo, Ching-Hsien Hsu(2021) proposed “Classification Based Machine Learning for
Detection of DDoS attack in Cloud Computing”
Disseminated Denial of administration attack(DDoS)is an organization security assault and presently the aggressors meddled into pretty much every innovation, for example, distributed computing, IoT, and edge figuring to make themselves more grounded. According to the way of behaving of DDoS, every one of the accessible assets like memory, computer processor or may be the whole organization are consumed by the aggressor all together to closure the casualty's machine or server. However, the bounty of cautious instrument are proposed, yet they are not proficient as the aggressors get themselves prepared by the recently accessible mechanized going after apparatuses. In this way, we proposed an order based AI approach for recognition of DDoS assault in distributed computing. With the assistance of three grouping machine learning calculations K Nearest Neighbor,

Random Forest and Gullible Bayes, the component can distinguish a DDoS assault with the precision of 99.76%

Ajeetha G, Madhu Priya G (2019) proposed "Machine Learning Based DDoS Attack Detection",Disseminated forswearing of administration assault has more
risk particularly in the field of digital protection. The DDoS assault generally emerges from the application layer or the organization layer where the casualties framework and the assailants framework are interconnected in an organization. The impacts of these assaults may change from making critical disappointments at the pointed servers making burden for clients utilize a specific help. The DDoS assault brings notoriety harm, efficiency misfortune, income misfortune, and even robbery for gigantic business firms and furthermore for banking areas. Thus there is a requirement for a decent disseminated forswearing identification and anticipation procedure. The significant objective is to convey ideal answer for these issues utilizing highlight investigation. At the point when a weighty traffic stream is experienced at the designated server, it is essential to group them as an assault or genuine access. In this way a book strategy has been proposed for the discovery of Distributed forswearing of administration assaults through the follows in the rush hour gridlock stream. A disarray framework has been produced from these follows. Two classifiers to be specific Naive Bayes and Random Forest are utilized to arrange the traffic as strange or typical, utilizing the typical also, assault profile got from existing datasets. Innocent Bayes calculation gives improved results than Random Forest calculation.

Mahdi Hassan Aysa, Abdullahi Abdu Ibrahim, Alaa Hamid Mohammed (2020) proposed "IoT DDOS ATTACK DETECTION USING MACHINE LEARNING" The conveyance technique of a botnet essentially coordinates its setup, introducing a help of bots for coming abuse. In this article, we use the wellsprings of pandemic displaying to IoT networks comprising of WSNs. We fabricate a proposed system to recognize and unusual protection exercises. As indicated by the effect of IoT-explicit elements like deficient handling power, power restrictions, and hub thickness on the development of a botnet, there are critical difficulties. We utilize standard datasets for dynamic two well known assaults, like Mirai. We additionally utilized quite a large number AI and information mining calculations like LSVM, Brain Network, and Decision tree to recognize strange exercises, for example, DDOS highlights. In the trial results, we found that the converge between irregular timberland and choice tree accomplished high exactness to distinguish assaults.

Marwane Zekri, Said El Kafhali, Noureddine Aboutabit and Youssef Saadi (2017) proposed "DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments" Distributed computing is an upset in IT innovation that gives versatile, virtualized on-request assets to the end clients with more noteworthy adaptability, less upkeep and decreased framework cost. These assets are managed by various the board associations and gave over Internet utilizing known systems administration conventions, norms and arrangements. The fundamental advancements and heritage conventions contain bugs and weaknesses that can open entryways for interruption by the assailants. Assaults as DDoS (Distributed Denial of Service) are ones of the most regular that incur genuine harm and influence the cloud execution. In a DDoS assault, the assailant normally utilizes guiltless compromised PCs (called zombies) by taking benefits of known or obscure bugs and weaknesses to send an enormousnumber of bundles from these generally caught zombies to a server. This might possess a significant part of organization transmission capacity of the casualty cloud foundations or consume a significant part of the servers time. Consequently, in this work, we planned a DDoS identification framework in light of the C.4.5 calculation to relieve the DDoS danger. This calculation, combined with signature identification strategies, creates a choice tree to perform programmed, successful identification of marks assaults for DDoS flooding assaults. To approve our framework, we chose other AI methods and looked at the got results.

Swathi Sambangi * and Lakshmeeswari Gondi *(2020) proposed "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection in WebServer."The issue of recognizing Distributed Denial of Service (DDos) assaults is generally an order issue in AI. In importance to Cloud Computing, the errand of ID of DDoS assaults is a fundamentally difficult issue as a result of computational intricacy that must be tended to. Essentially, a Denial of Service (DoS) assault is a purposeful assault endeavored by assailants from single source which has a certain expectation of making an application inaccessible to the objective partner. For this to be accomplished, aggressors as a rule stun the organization transmission capacity, ending framework assets, consequently causing disavowal of access for real clients. As opposed to DoS assaults, in DDoS assaults, the aggressor utilizes various sources to start an assault. DDoS assaults are generally normal at network, transportation, show and application layers of a seven-layer OSI model. In this paper, the examination objective is to concentrate on the issue of DDoS assault identification in a Cloud climate by considering the most famous CICIDS 2017 benchmark dataset and applying numerous relapse investigation for building an AI model to anticipate DDoS and Bot assaults through considering a Friday evening traffic logfile.

Kriti Bhushan, B. B. Gupta (2018) proposed "Detecting DDoS Attack using Software Defined "Network (SDN) in Cloud Computing Environment" Over the most recent multi decade, distributed computing has advanced as a new and promising computational stage that gives practical and versatile processing office. The consolidation of SDN innovation with the distributed computing climate rearranges the cloud's organizing intricacies and essentially works on the reasonability, programmability, dynamism, and versatility of the cloud. In the SDN-based cloud, the fundamental elements of SDN, counting worldwide perspective all in all organization, programming based traffic investigation, brought together command over the organization, and so forth

extraordinarilyfurther develops the DDoS assault discovery and moderation abilities of the cloud. In this paper, we initially examine about different fundamental elements of SDN that makes it reasonable systems administration innovation for distributed computing. Also, we propose a way to deal with distinguish DDoS assaults in SDN-based cloud by using the highlights of SDN. The proposed approach can recognize the DDoS assaults with exceptionally low communicational and computational upward. Our claims are all around upheld by the broad recreation based tests.

SHI DONG AND MUDAR SAREM(2019) proposed "DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks",The Distributed Denial of Service (DDoS) assault has truly disabled network accessibility for a really long time yet there is no successful safeguard system against it. Be that as it may, the arising Software Dened Networking (SDN) gives a newway to reexamine the protection against DDoS assaults. In this paper, we propose two strategies to distinguish the DDoS assault in SDN. One strategy takes on the level of DDoS assault to distinguish the DDoS assault. The other technique utilizes the superior K-Nearest Neighbors (KNN) calculation in light of Machine Learning (ML) to find the DDoS assault. The consequences of the hypothetical examination and the exploratory outcomes on datasets demonstrate the way that our proposed strategies can more readily recognize the DDoS assault thought about with different strategies.

Diash Firdaus,Rendy Munadi,Yudha purwanto(2020) proposed" DDOS Attack Detection in Software Defined Network using Ensemble K-means++ and Random Forest"

SDN (Software Defined Network) is the future of systems administration and has drawn in extraordinary interest as another worldview in S in systems administration. SDN has unified control by isolating control plane and information plane, it will be truly powerless against DDoS assaults. To further develop security, it requires high discovery precision and productivity. To identify DDoS assaults on SDN we propose DDoS discovery utilizing Machine Learning with Ensemble Algorithm. At the trial stage, we utilized In SDN as a dataset. This study comprises of two strategies. The initial step is the grouping and arrangement technique, the bunching and order strategy has two phases, the main stage is highlight choice and standardization, and the subsequent stage is Ensemble Algorithm bunching and characterization. The subsequent advance is the location approval technique in SDN utilizing the Mirinet emulator. We use Ensemble Algorithm K-means++ and Random Forest to ob tain High identification exactness and effectiveness.

III. METHODOLOGY

Slowly Increasing Polymorphic DDOS Attack Strategy (SIPDAS)

To Detect low-rate assaults and forestall Dos utilizing SIPDAS. We compute the twofold auto-relationship (DA) coefficient series and look at the principal Nmax components in such series. On the off chance that the conduct in the pattern part has a clear expanding or declining propensity, then those Nmax values will all surpass a specific limit. Distributed computing permits clients to get to cloud assets and administrations. On-request, self-administration and pay-by-use plan of action are adjusted for the cloud asset sharing cycle. Administration level arrangements (SLA) manage the expense for the administrations that are accommodated the clients. Cloud server farms are utilized to share information values to the clients. Disavowal of-Service (DoS) assault is an Endeavor by aggressor to keep authentic clients from utilizing assets. Disseminated Denial of Service (DDoS) Attacks are produced in a "numerous to one" aspect. In DDoS assault model large number of compromised have are assembled to send futile assistance demands, bundles simultaneously. DoS and DDoS assaults starts the help debasement, accessibility, and cost issues under cloud specialist co-ops.

Beast force assaults are raised against through unambiguous occasional, beating, and low-rate traffic designs. Rate-controlling, time-window, most pessimistic scenario edge and example matching are adjusted to separate the genuine and aggressor exercises. Secretive assault designs are brought against applications running up in the cloud. Gradually Increasing-Polymorphic DDoS Attack Strategy (SIPDAS) can be applied to start application weaknesses. SIPDAS debases the assistance given by the objective application server running in the cloud. Polymorphic assaults changes the message arrangement at each progressive disease to keep away from signature discovery process. Gradually expanding polymorphic way of behaving initiates an adequate number of over-burdens on the objective framework. XML-based DoS (XDoS) assaults to the online frameworks are applied as the testing climate for the assault identification process.

IV. ARCHITECTURAL DIAGRAM

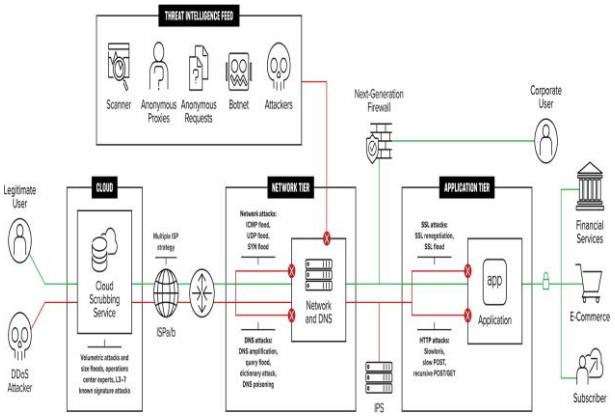

Fig 2: DDOS Prevention Architectural Diagram

A multi-layered DDoS insurance engineering

F5 suggests a half breed cloud/on-premises DDoS arrangement. Volumetric assaults will be relieved by F5 Silverline DDoS Protection — a help conveyed by means of the F5 Silverline cloud-based stage. Silverline DDoS Protection will investigate and eliminate the majority of assault traffic.

Some of the time, a DDoS mission might incorporate application layer goes after that should be tended to in the vicinity. These deviated and computational assaults can be alleviated utilizing the organization safeguard and application protection levels. The organization safeguard level is made out of L3 and L4 network firewall administrations and straightforward burden adjusting to the application protection level. The application safeguard level comprises of more modern (and more CPU-concentrated) administrations including SSL end and a web application firewall stack. There are convincing advantages to isolating organization guard and application protection for the on-premises piece of the DDoS Protection design.

The organization and application protection levels can be scaled autonomously of each other. For instance, when web application firewall use develops, another apparatus (or edge) can be added to the application level without influencing the organization level.

The organization and application safeguard levels can utilize different equipment stages and, surprisingly, unique programming renditions.

At the point when new strategies are applied at the application safeguard level, the organization protection level can guide just a part of traffic to the new approaches until they are completely approved.

V. ACTIVITY DIAGRAM

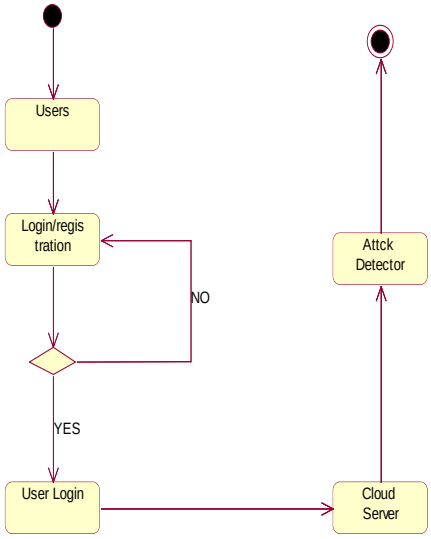

Fig 3: Activity Diagram

VI. ALGORITHM

- Step 1: User Interface Design- Cloud User inputs values Login name and Password. If Valid cloud user, it opens the user window otherwise displays error page.
- Step 2: Admin Upload-After login admin can be able to upload the files in the cloud and user can able to view the file and user can able to download files.
- Step 3: Admin security key-Before uploading files in the cloud admin should be able to enable the security key to prevent the DOS Attacks.
- Step 4: Attacker Login-Attacker can be able to login into the cloud and able to attack the entire cloud. When security key is disable, attacker can easily attack the cloud.
- Step 5: Predicting Future Attacks (ML) - By gathering past datasets by using supervised learning we can able to predict the future attacks and prevent the attacks in the month where on that time admin can enable the security key.

VII. PERFORMANCE EVALUATION

The dataset picked for trial and error comprised of five-day log records from Monday to Friday in csv design. For try investigation, we have considered the log record of Friday evening which additionally comprised of two class marks. The class names are Benign (Normal) and DDoS (assault). The complete number of traffic bundles in the log record included 225,746 traffic parcels.

Explore Analysis for the Log File of Friday Afternoon with Class Labels as Benign (Normal) and DDoS (Attack)

At first, the quantity of qualities in the Friday evening logfile are 78 with the last characteristic being the class name, i.e., there are 79 aspects alongside class mark. At first, the displaying system began by use of element determination calculation which depends on calculation of data gain for every one of the qualities in the dataset. The main 16 ascribes have been considered for maintenance and different traits in the characteristic set are taken out. Figure3depicts the whole subtleties of ANOVA model and the rundown of the main 16 ascribes with higher data gain are recorded in Figure4. For numerical displaying, we decided to play out different straight relapse investigation by running relapse examination on the logfile with these 16 credits. After introductory examination is conveyed, the traits that are held incorporate the characteristics at aspects 1, 5, 6, 7, 9, 11, 13, 35, 36, 53, 54, 55, 56, 64,66 and 67. The examination is in this way performed utilizing the diminished dimensionality log record with these 16 credits as referenced previously. The mean outright rate mistake for the straight relapse model is acquired as 0.2621. Consequently, the rate exactness of the various straight relapse model is acquired as equivalent to 73.79%, i.e., 0.7379.

Figure5shows the lingering plot got for every one of the 16 credits of the CICIDS 2017 dataset
w.r.t Friday evening log document. Figure6shows the leftover plot and Figure7shows the fit graph for the by and large different direct relapse model. After the underlying model is grown, then, we have dispensed with 10 credits which are not genuinely critical and held the excess six attributes. In this way, the quantity of qualities is presently decreased to six attributes. The property aspects are 1, 9, 13, 53, 54, and 64. Yet again then, the different relapse examination is performed on these measurably huge properties. Figure8depicts the fit diagram, envisioning the real name and anticipated mark. Figure9shows these six ascribes' lingering plots lastly, Figure10depicts the remaining plot for the model. In this way, the AI model precision acquired utilizing these six ascribes is 71.6% which likewise plainly shows that the principal model with 16 credits is nearly better.

ANOVA

	df	SS	MS	F	Significance F
Regression	16	29778.18946	1861.136841	23832.54328	0
Residual	225733	25640.72297	0.113588722		
Total	225749	55418.91243			

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%	Upper 95.0%
Intercept	1.48016318 1E0	1.214964E-3	1.21827737E3	0	1.47778188 3E0	1.48254448E0	1.47778188 3E0	1.48254448E0
Destination Port	-7.9586E-06	5.07513E-08	-1.568157955E2	0	-8.05807E-06	-7.85913E-06	-8.05807E-06	-7.85913E-06
Total Length of Fwd Packets	0	0	6.5535E4	#NUM!	0	0	0	0
Total Length of Bwd Packets	3.09845E-06	6.49544E-08	4.77018338E1	#NUM!	2.97114E-06	3.22576E-06	2.97114E-06	3.22576E-06
Fwd Packet Length Max	8.64604E-06	1.1702E-06	7.38850599 2E0	1.48996E-13	6.35248E-06	1.09396E-05	6.35248E-06	1.09396E-05
Fwd Packet Length Mean	0	0	6.5535E4	#NUM!	0	0	0	0
Bwd Packet Length Max	2.86673E-06	7.00377E-07	4.09312606 3E0	#NUM!	1.49401E-06	4.23945E-06	1.49401E-06	4.23945E-06
Bwd Packet Length Mean	7.06531E-05	3.26813E-06	2.16188072 3E1	1.5235E-103	6.42476E-05	7.70585E-05	6.42476E-05	7.70585E-05
Fwd Header Length	0	0	6.5535E4	#NUM!	0	0	0	0
Bwd Header Length	-5.97066E-4	5.71258E-06	-1.045177417E2	#NUM!	-6.08262E-4	-5.85869E-4	-6.08262E-4	-5.85869E-4
Average Packet Size	2.81867E-4	4.07743E-06	6.91284760 6E1	0	2.73875E-4	2.89858E-4	2.73875E-4	2.89858E-4
Avg Fwd Segment Size	-1.49379E-4	4.89145E-06	-3.053887974E1	2.0805E-204	-1.58966E-4	-1.39792E-4	-1.58966E-4	-1.39792E-4
Avg Bwd Segment Size	0	0	6.5535E4	#NUM!	0	0	0	0
Fwd Header Length	4.1925E-4	7.04326E-06	5.95249305 4E1	#NUM!	4.05445E-4	4.33054E-4	4.05445E-4	4.33054E-4
Subflow Fwd Bytes	-3.81369E-06	4.82535E-07	-7.90345282 7E0	2.72494E-15	-4.75944E-06	-2.86793E-06	-4.75944E-06	-2.86793E-06
Subflow Bwd Bytes	0	0	6.5535E4	#NUM!	0	0	0	0
Init_Win_bytes_forward	-1.24761E-05	9.91958E-08	-1.25772791 1E2	#NUM!	-1.26706E-05	-1.22817E-05	-1.26706E-05	-1.22817E-05

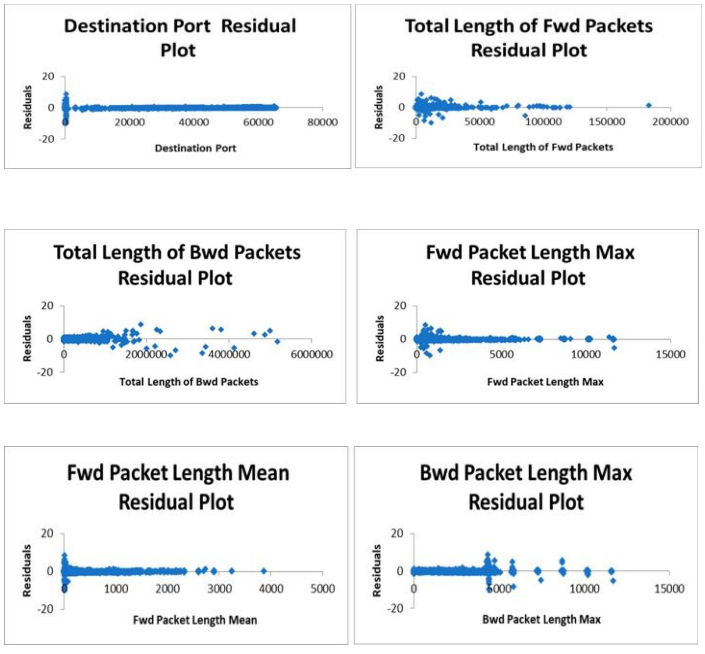

Fig 4. Cont.

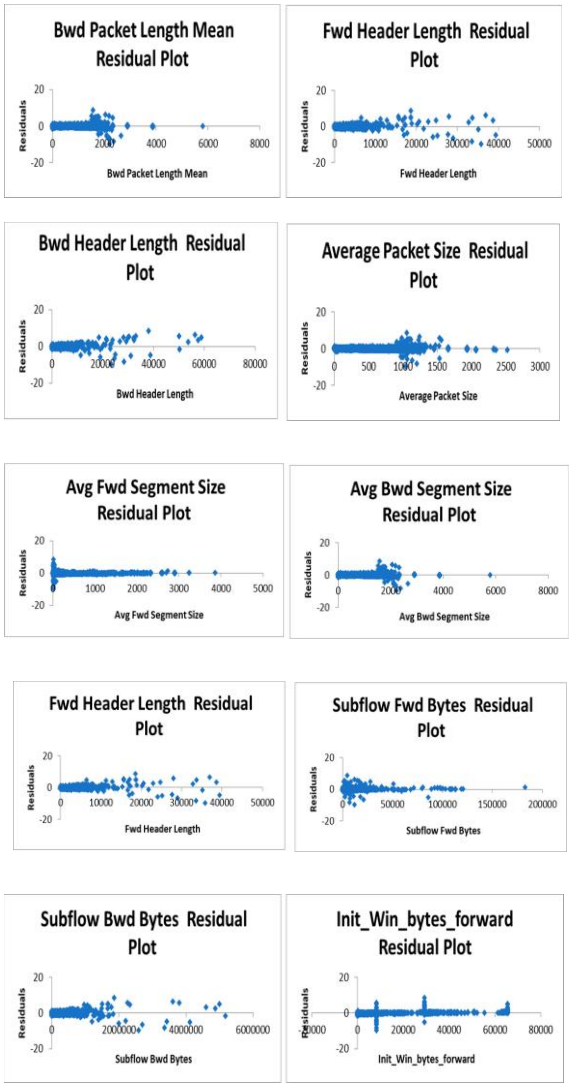

Figure 5. Residual plots for 16 attributes of Friday afternoon log of CICIDS 2017 dataset.

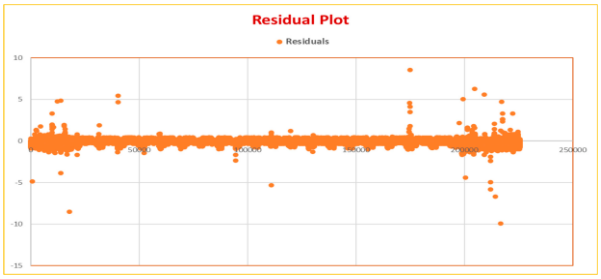

Fig 6. Residual plot obtained for multiple linear regression model for CICIDS 2017 dataset

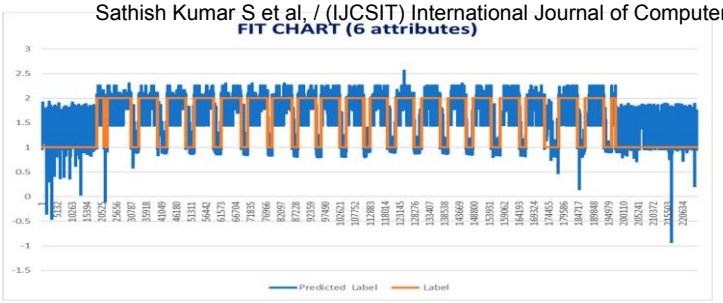

Fig 7. Fit chart obtained for Friday afternoon logfile of CICIDS 2017 dataset by considering 1, 9, 13, 53, 54, and 64 attributes.

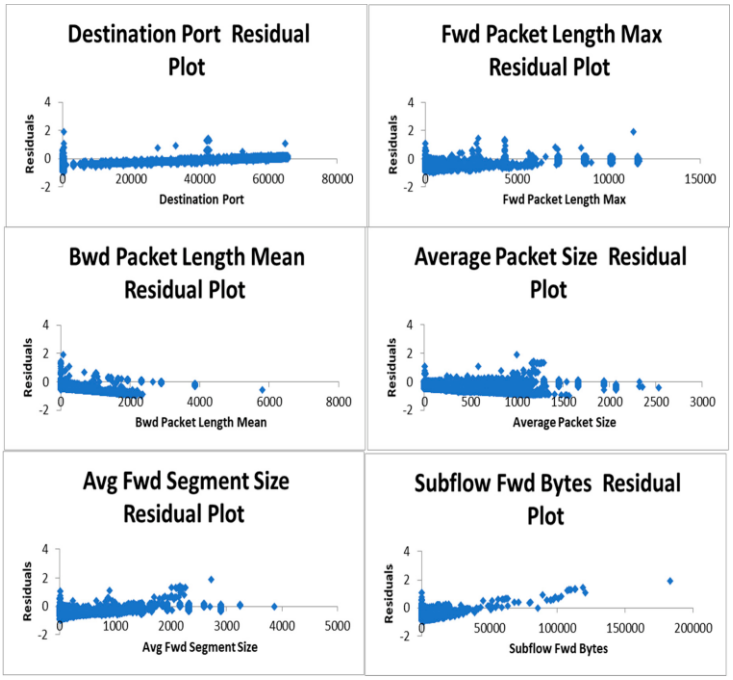

Fig 8. Residual plots for six attributes of Friday afternoon log of CICIDS 2017 dataset

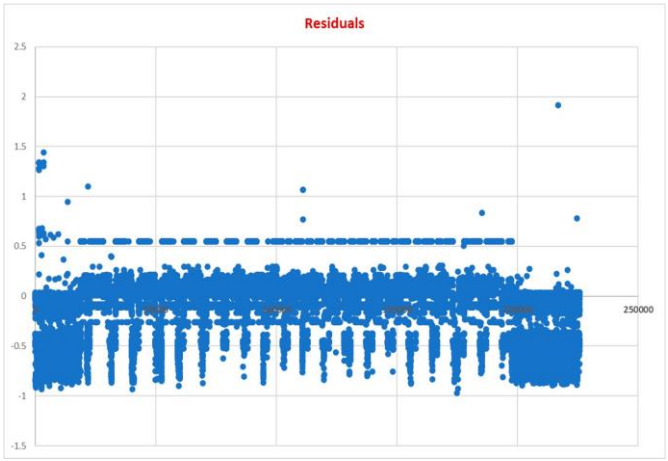

Figure 10. Residual plot obtained for multiple linear regression model for CICIDS 2017 dataset by considering six attributes of the dataset.

VIII. REFERENCE

1) Firdaus, D., Munadi, R., & Purwanto, Y. (2020). DDoS Attack Detection in Software Defined Network using Ensemble K-means++ and Random Forest. 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). doi:10.1109/isriti51436.2020.9315521

2) Zhijun, W., Jingjie, W., & Meng, Y. (2018). Prevention of DoS Attacks in Information-Centric Networking. 2018 IEEE Conference on Application, Information and Network Security (AINS). doi:10.1109/ains.2018.8631473

3) M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.

4) F. Cheng and C. Meinel, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729–734.

5) C. Metz. (2009, Oct.). DDoS attack rains down on Amazon Cloud [Online]. Available:http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/S

6) K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," Comput. Netw., vol. 51, no. 18, pp. 5036–5056, 2007.

7) H. Sun, J. C. S. Lui, and D. K. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in Proc. 12th IEEE Int. Conf. Netw. Protocol., 2004, pp. 196-205.

8) A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-Targeted denial of service attacks: The shrew vs. the mice and elephants," in Proc. Int. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2003, pp. 75–86.

9) M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of quality (RoQ) attacks on internet end-systems," in Proc. IEEE Int. Conf. Comput. Commun., Mar. 2005, pp. 1362 1372.

10) X. Xu, X. Guo, and S. Zhu, "A queuing analysis for low-rate DoS attacks against application servers," in

Proc. IEEE Int. Conf. Wireless Commun., Netw. Inf. Security, 2010, pp. 500–504.

11) L. Wang, Z. Li, Y. Chen, Z. Fu, and X. Li, "Thwarting zero-day polymorphic worms with network-level length-based signature generation," IEEE/ACM Trans. Netw., vol. 18, no. 1, pp. 53–66, Feb. 2010.

12) A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defense to protect cloud computing against HTTP-DOS and XMLDoS attacks," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1097–1107, Jul. 2011.

13) D. Petcu, C. Craciun, M. Neagul, S. Panica, B. Di Martino, S. Venticinque, M. Rak, and R. Aversa, "Architecturing a sky computing platform," in Proc. Int. Conf. Towards Serv.-Based Int., 2011, vol. 6569, pp. 1-13.

14) U. Ben-Porat, A. Bremler-Barr, and H. Levy, "Evaluating the vulnerability of network mechanisms to sophisticated DDoS attacks," in Proc. IEEE Int. Conf. Comput. Commun., 2008, pp. 2297–2305.

15) S. Antonatos, M. Locasto, S. Sidiroglou, A. D. Keromytis, and E. Markatos, "Defending against next generation through network/ endpoint collaboration and interaction," in Proc. IEEE 3rd Eur. Int. Conf. Comput. Netw. Defense, 2008, vol. 30, pp. 131–141.

16) R. Smith, C. Estan, and S. Jha, "Backtracking algorithmic complexity attacks against a NIDS," in Proc. Annu. Comput. Security Appl. Conf., Dec. 2006, pp. 89–98.

17) C. Castelluccia, E. Mykletun, and G. Tsudik, "Improving secure server performance by re-balancing SSL/TLS handshakes," in Proc. ACM Symp. Inf., Apr. 2005, pp. 26–34.