Machine Learning to Detect and Mitigate DDoS Attacks on SDN

D G Tejas , T N R Kumar

Department of Computer Science,
M S Ramaiah Institute of Technology,India
e-mail:tejasdg966@gmail.com,tnrkumar@msrit.edu

Abstract

SDN (software defined networking) offers a number of benefits, such as innovation, monitoring, and flexibility. SDNs are susceptible to a variety of security risks, though. Distributed Denial of Service (DDoS) attacks are one of the primary forms of attacks that interfere with SDN networks. DDoS attacks can be prevented in a variety of ways on SDN networks. DDoS attacks can be recognised and avoided using machine learning techniques like Naive Bayes, Support Vector Machines (SVMs), and MLP classifier. The RYU controller must be trained as part of this procedure, and records of regular and attack traffic must be made. When the controller is in detection mode, it invokes the machine learning algorithm to identify the kind of traffic using a sample of the traffic that was input from one of the hosts.Blocking the host MAC address in attack scenario lessens the attack. The results demonstrated that the MLP classifier outperforms the other tested algorithms.

Keywords - Distributed Denial of Service (DDoS), Machine learning,MLP classifier, Naive Bayes, Support Vector Machines (SVMs), Software defined networking (SDN)

1. INTRODUCTION

Because of its benefits in terms of monitoring, scalability, and flexibility, software defined networking (SDN) is widely used today[1]. Traditional network devices combine control and data planes, but SDNs have a separate control plane from the data planes[2]. This is the primary distinction between traditional networks and SDNs. Network components like switches and routers are found in the data plane and are controlled by the controller in the control plane[3]. Network management is made simpler by the controller's handling of configuration and management[1][2]. To make network upgrades and repairs, administrators don't have to log into and reset a sizable number of devices on the network. Easily integrate real-time policy applications and network applications from the controller[4].The difference between a traditional network and SDN is depicted in Fig. 1.

To run the data plane, the controller needs to use a few basic services. In order to offer network tasks like routing, load balancing, and access detection[1], it can communicate data with application layer services. To provide the highest level of network management, computerization, and proficiency, every one of the administrations and programmes used in the application layer are planned throughout the network using the operating system installed on the controller[1].

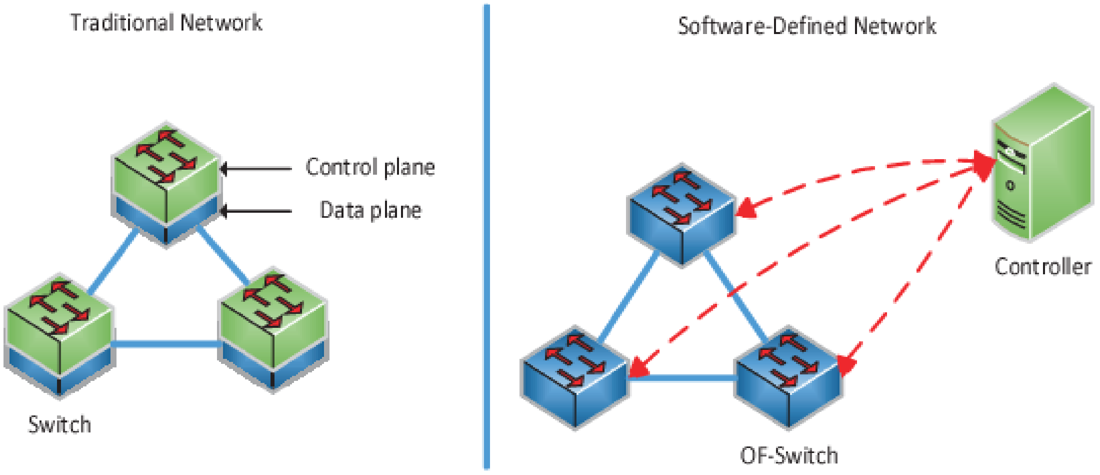

Fig 1: Difference between traditional network and Software Defined Network

Applications use application programming interfaces (APIs), such as Java API for close communications with the controller or Representational State Transfer (REST) API for distant communications with the controller[3]. As a result, Fig. 2 shows the SDN's design.

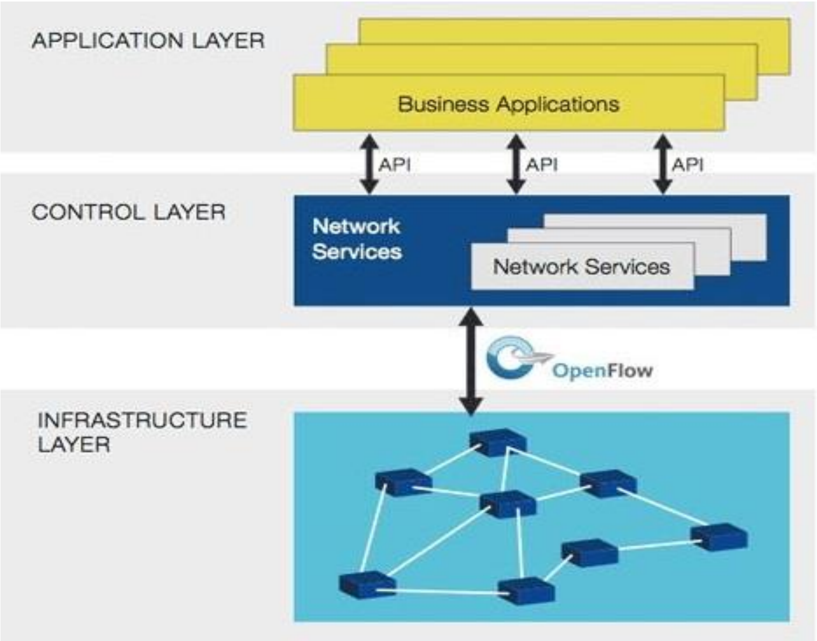

Fig 2: SDN Architecture

DDoS attacks, in any case, severely harm SDN networks. In the unlikely event that the network is not properly secured, a DDoS attack may defeat the OpenFlow (OF) switch or control data transit. To protect SDN networks from DDoS attacks, there are numerous records. One such cutting-edge technology that attracts experts is focused on using machine learning to identify DDoS attacks. However, protecting SDN networks from threats continues to be a valid research subject. This article focuses on a method for identifying DDoS attacks on active networks and selecting the best machine learning algorithm to mitigate them.

2. Necessity of SDN for various applications

Security Services : Particular virtual services running at the network layer are supported by today's virtualization environment. To do this, SDN platforms must have features like NFV. With the help of this kind of network security, risk may be reduced and events can be handled much more rapidly. Every second counts in halting an attack when there is a breach. The ability to recognise the attack and make sure that other network components are secure is also crucial. Attacks and sophisticated advanced persistent threats will increase as the network layer becomes progressively more crucial and as the modern business becomes even more digital. A more proactive environment that can adapt to change is made possible by including strong security services into the SDN layer.

Network Intelligence and Monitoring : The network layer, one of the data center's most important levels, is being abstracted by modern SDN technologies. More data must be handled by network designs than ever before, which makes them considerably more complicated. Knowing what is permeating your environment is therefore essential. Are there latency problems on a port? What if your network design is heterogeneous? Or, do you use a lot of virtualization and send a lot of data across the network layer? When you have a strong network intelligence and monitoring layer, all of these problems disappear. However, by incorporating these technologies into your SDN design, you get real insight and advantage. Network intelligence and monitoring tools may incorporate traffic flow, port settings, hypervisor integration, alerts, and even optimization.The ability to better monitor network traffic between your data centre and your cloud environment is what these agile system types are most useful for.

Compliance and Regulation-Bound Applications : The capacity to store and manage workloads that are subject to compliance is increasingly being offered by major cloud suppliers. Organizations now have the choice to expand designs that were previously quite constrained in dispersed systems and the cloud due to laws. However, how do you divide the traffic? How can you guarantee that tasks related to compliance and regulation are consistently safeguarded and monitored? SDN can be useful here. An SDN architecture allows for the management of network traffic between switches, network nodes, and even hypervisors. Keep in mind that this layer isolates hardware controllers and virtual functionalities. Then, this robust layer can reach several places, virtualization nodes, and even cloud locations.

High-Performance Applications:New application technology categories are proliferating right now. Rich applications like GIS, CAD, engineering, and graphics design tools may now be delivered thanks to virtualization. These workloads have often required bare-metal systems with separate connections. In contrast, virtualization allows for the streaming of apps and the creation of sophisticated desktop environments through VDI. However, we also observe the incorporation of SDN into application control at the network layer. establishing strong QoS regulations, protecting private information, dividing up heavy traffic, and even establishing threshold alarms around bottlenecks. All of these SDN capabilities facilitate the delivery of rich, high-performance applications through virtualization.

Distributed Application Control and Cloud Integration : The ability of SDN to expand over the whole data centre is one of its greatest advantages. Distributed locations, the cloud, and the entire business are all integrated by this form of agility. Regardless of the underlying network architecture, SDN enables the transfer of vital network traffic across diverse locations. Data flow between data centre and cloud locations is made simpler by abstracting crucial network controls. Because SDN is a type of network virtualization, you can utilise powerful APIs to manage certain network functions in addition to integrating with a cloud provider. This enables you to control your workloads precisely while maintaining the flexibility of your company.

3. DDoS CLASSIFICATIONSANDFEATURES

3.1DDoSClassification

DDoS attacks, as previously said, aim to inundate a target organisation with a huge number of packets from multiple locations. DDoS attacks have many different techniques to flood the victim network, including the use of botnets, arbitrary IP flood attacks, TCP, UDP, and ICMP flood attacks.

3.1.1 TCPFlood

TCP flood attacks are the most well-known DDoS attacks. TCP flood attacks repeatedly send TCP association requests to the victim without really inspecting the victim's server's SYN-ACK. The casualty's server has a lot of open connections that are quite active. This fictitious association uses up all or a significant portion of the resources, rendering them unavailable to actual clients[6].

3.1.2 ICMPFlood

Smurf attacks, also known as ICMP flood attacks, are another type of DDoS. Send an absurdly large amount of ICMP packets using the mock IP address to the victim. A dishonest IP address holder receives an ICMP response from the casualty's server. This affects the appearance and usability of the victim's server as well as the legitimate owner of the fictitious IP address[6].

3.1.3 UDPFlood

UDP flooding is the third type of DDoS attack. They piled mountains of UDP packets inside the casualty. The infiltration of DNS intensification is one such model. The attacker in this attack mistook the victim's IP address and made a quick query to the DNS server. The DNS server responds with a massive response that degrades the casualty's appearance. In order to prevent it from happening to regular customers, UDP flooding can also be caused by flooding the victim with a large number of UDP bundles[6].

3.1.4 RandomIPFlood

DDoS attacks can also start by creating erroneous IP bundles, which prevents the controller from responding to other legitimate traffic since it is too busy dealing with untidy packets[4]. SuccessfulDDoS attacks can take the majority of the day to accumulate large numbers of malicious bundles and can occur at specified times[2].

3.1.5Botnets

A botnet is a bizarre and perilous DDoS attack tactic. Botnets are a sizable collection of vulnerable PCs[5]. Some easy-to-use attack-creating tools are available for free or at very low cost. Without a doubt, anyone can locate assets or enlist the help of others to carry out a variety of online attacks. Botnets are operated by installing malicious software on your computer using dubious methods. Phishing scams, spam messages, website connections, or downloads from unknown clients can all do this. An infected PC is used by a malware application to communicate with the botnet owner's command and control system (O&C). The O&C server then uses distributed correspondence and collaboration to transmit instructions to every compromised PC (about thousands of them) in an effort to harm the victim's organization's server.

4. Problem with SDN

DDoS attacks are the most frequent yet terrifying attacks on SDNs. Such attacks have an impact on how the network is presented and operated. They are impairing or degrading network services by shutting down apps, and legitimate clients are unable to communicate with the SDN controller or deliver packages across the network[9].

By creating a few new flows that flood the controller bandwidth, OpenFlow switches, and SDN controls, DDoS attacks against SDNs are carried out, resulting in network disappointments for genuine hosts. Evidently, the attackers are producing a few new flows that were delivered from various sources but had harmed IP addresses (DDoS). There is a table disappointment since these casualty addresses don't correspond to any of the principles that are currently included in the OpenFlow switch flow table. Due to this situation, large packet messages are generated and sent from the OpenFlow switch to the SDN controller, using up network bandwidth, memory, and CPU for both control and flight of the SDN data[10]. Additionally, since the OpenFlow switch cradles each message before delivering it to the controller, if too few fresh flows are detected in a short period of time, the capacity is exhausted. In contrast to delivering header-less package header messages only sometimes, this results in sending all new flowpackets to the controller, increasing utility bandwidth management and delaying the establishment of new flow rules established in the SDN controller.

The OpenFlow switch forwarding table being fully filled is another factor that can create a significant amount of problem. As previously said, the controller reviews and keeps an eye on a table that includes a variety of flow rules that supervise the change in terms of packetmove[11].New flow rules are displayed in the flow table when there are a few new flows. Sometimes, the flow table becomes full, making it impossible to incorporate new flow rules when they are received from the controller. As a result, it discards the bundle and notifies the controller of the error[12]. Additionally, the switch delays and scales down approaching packages since it cannot move packages until its sending table has free memory[13].

The heightened level of internal package message appearance that exceeds the controller's handling capacity frustrates the controller and blocks access to actual traffic on the controller's side. As the controller uses SDN intelligence and manages OpenFlow applications and switches, this could result in the network as a whole experiencing disappointment[13]. Figure 3 provides a clear perspective on DDoSattacks on SDNs.

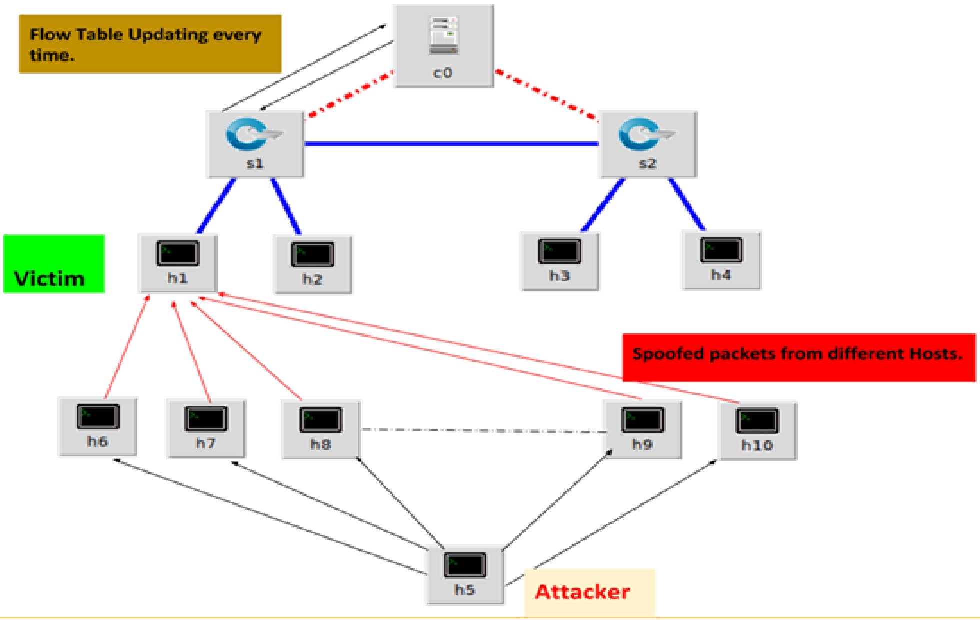
Flow Table Updating every time.
c0
s1
s2
Victim
h1
h2
h3
h4
Spoofed packets from different Hosts.
h6
h7
h8
h9
h10
h5
Attacker

Fig 3: DDoS attack on SDN

5. SDNDDOSDETECTION ANDMITIGATION MODEL

The experiment is run on Ubuntu (20.4) and a virtual machine with 4GB of RAM and 40GB of hard drive space is set up in VMware. SDN networks are created using Mininet (2.3) and the RYU controller (4.3). Switch 2 (S2) is connected to four hosts (h1, h2, h3, and h4), and Switch 3 (S3) is connected to servers 1 and 2 (h5 and h6) (S3). Switch 1 is connected to S2 and S3 (S1). S1 belongs to the RYU controller. In Fig 4, the topology is shown.

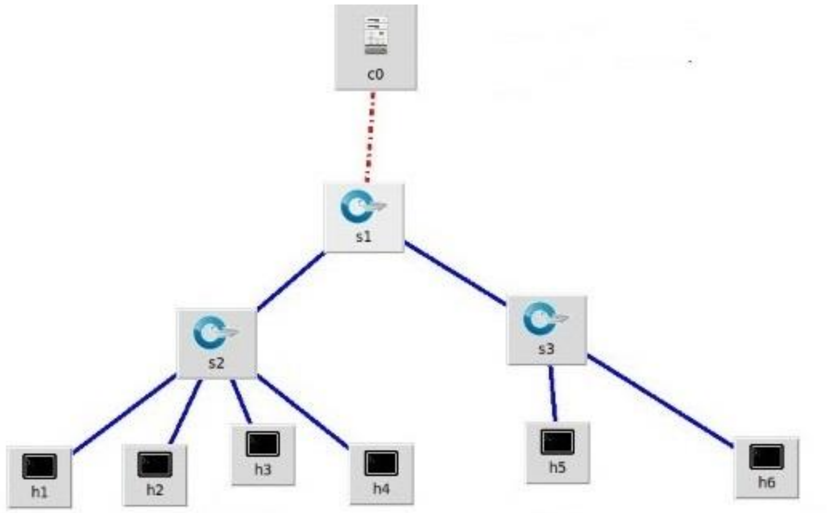

Fig4: Topology of the network

The suggested system makes use of four contents:

- Common Traffic Scripts - Distribute all hosts and servers with randomly generated HTTP and ICMP packages.
- DDoS Traffic Script - Floods ICMP and TCP packets to the web server at a rate of 100 packets per second while using a source IP that is mocked and hastily generated using hping3.
- Detection Script - Groups approaching OF switch bundles into DDoS packets and regular packets using the selected MLP classifier.
- Mitigation Script - Block the port used by the DDoS aggressor on the OF switch and add a flow section through the controller using REST messages.

5.1 TrainingandTestingDataset

The host generates custom and DDoS traffic scripts while the controller is in collection mode to provide the training dataset. Python code has used the hping3 programme to deploy common DDoS packs (ICMP and TCP floods). DDoS and regular traffic were taken separately to prevent chaos while creating informational indexes. 100packets were added to the DDoS flow every second for 15 minutes. After the DDoS examination was complete, regular traffic was used for 15 minutes to measure the DDoS value and regular traffic.

Catch data is stored in a CSV file to omit significant highlights and exclude unnecessary data, such as Address Resolution Protocol (ARP). The main goal of this research is to identify and mitigate DDoS on SDN networks using machine learning. Therefore, you should use a component that can be easily removed without placing an undue stress on the network. The training dataset yielded the accuracy scores for Naive Bayes, Support Vector Machines (SVMs), and MLP classifiers, which are displayed in TABLE I. Since they are quicker and simpler to construct, we focused on the information highlights shown in [8] in order to achieve our goal.

Machine Learning Algorithm	**Accuracy(%)**
Support Vector Machines (SVMs)	96.73
GuassianNaive Bayes	99.85
MLP classifier	100

TABLEI.Comparison betweenNaïve Bayes,SVM andMLP classifier

The Guassian Naive Bayes, SVM, and MLP classifiers were compared analytically, and the results are presented in TABLE I. It was determined that the MLP classifier, due to its high accuracy, is best suited for our situation. In our SDN network, we kept the MLP classifier to be utilised for classifying both online DDoS and regular network traffic.

5.2 Experimental Results

The controller runs in two modes. collection mode and detection mode. When the controller is in collection mode, the host generates Customary traffic scripts and DDoS traffic scripts to create the machine learningdataset. When the controller is in detection mode, the host provides a pattern of incoming traffic and the controller invokes the machine learningalgorithm that uses the machine learning dataset to detect the type of traffic.For normal traffic, the controller's output prediction logic is 0, returning to flow monitoring. For attack traffic, the controller's output prediction logic is 1. This is a DDoS attack and means that the MAC address of the host that caused the DDoS attack is blocked and the controller returns to Monitor the flows.

6. Conclusion

In this study, we developed an SDN architecture that differentiates and protects the switches and controllers from DDoS attacks. This structure includes gathering data to develop machine learning models that can predict DDoS attacks. The predictions are subsequently used in relief archives to support decisions made by the SDN network. We put the data to use by putting the Naive Bayes, SVM, and MLP classifiers to the test. The results of our experiments demonstrate that the MLP classifier is best for our network. By utilising extremely effective machine learning algorithms to decrease the number of packet separation processes, we can continue to minimise the time it takes to identify DDoS attacks in future work.

References

[1] "Toward an Optimal Solution Against Denial of Service Attacks in Software Defined Networks-ScienceDirect."[Online].Available:https://www.sciencedirect.com/science/article/pii/S0167739X18302930#bb40.[Accessed:30-Mar-2019].

[2] N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D.Choi,"Time-Based DDoS Detection and Mitigation for SDN Controller," in 201517 th Asia-Pacific Network Operations and Management Symposium, 2015,pp.550–553.

[3] C.Lin,C. Li,andK. Wang, "Setting Malicious Flow Entries Against SDN Operations: Attacks and Countermeasures," in 2018 IEEE Conference onDependableand SecureComputing, 2018,pp.1–8.

[4] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN Security forIoT-RelatedDeploymentsthroughBlockchain,"in2017IEEEConference on Network Function Virtualization and Software DefinedNetworks,2017,pp.303–308.

[5] J. Smith-perrone and J. Sims, "Securing Cloud, SDN and Large DataNetworkEnvironments from Emerging DDoS Attacks," in 2017 7thInternational Conferenceon Cloud Computing,DataScienceEngineering-Confluence,2017,pp.466–469.

[6] B. Zhang, T. Zhang, and Z. Yu, "DDoS Detection and Prevention Basedon Artificial Intelligence Techniques," in 2017 3rd IEEE InternationalConferenceonComputerandCommunications,2017,pp.1276–1280.

[7] S.Choudhuryand A. Bhowal, "Comparative Analysis of Machine Learning Algorithms along with Classifiers for Network Intrusion Detection," in 2015 International Conference on Smart Technologies and Management for Computing, Communication,Controls,EnergyandMaterials,2015,pp.89–95.

[8] M.H.Bhuyan, D.K. Bhattacharyya,and J.K.Kalita,"Towards Generating Real-life Datasets for Network Intrusion Detection," J Netw.Secur.,vol.17,pp.683–701,2015.

[9] Ombase P.M., Kulkarni N.P., Bagade S.T., Mhaisgawali A.V.Survey on DoS attack challenges in software defined networking Int. J. Comput. Appl., 173 (2) (2017), pp. 19-25

[10] G. Shang, P. Zhe, X. Bin, H. Aiqun, R. Kui, FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks, in: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 2017, pp. 1–9.

[11] Ahmad I., Namal S., Ylianttila M., Gurtov A.Security in software defined networks: A surveyIEEE Commun. Surv. Tutor., 17 (4) (2015), pp. 2317-2346

[12] R. Kandoi, M. Antikainen, Denial-of-service attacks in OpenFlow SDN networks, in: Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015, 2015, pp. 1322–1326.

[13] H. Wang, L. Xu, G. Gu, FloodGuard: A DoS attack prevention extension in software-defined networks, in: 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2015, pp. 239–250.

[14] Veeranki, S. R., & Varshney, M. (2022). *Comparative analysis of thyroid disease and predict them using machine learning techniques.* International Journal of Health Sciences, 6(S3), 11005–11014. https://doi.org/10.53730/ijhs.v6nS3.8459

[15] Veeranki, S. R., & Varshney, M. (2022). *Application of data science and bioinformatics in healthcare technologies.* International Journal of Health Sciences, 6(S4), 5394–5404. https://doi.org/10.53730/ijhs.v6nS4.10728

[16] Sreenivasa Rao Veeranki, Manish Varshney. (2022). *Trends and Application of Data Science in Bioinformatics*. Design Engineering, (1), 3541 - 3555. Retrieved from http://www.thedesignengineering.com/index.php/DE/article/view/950

[17] Sreenivasa Rao Veeranki, Manish Varshney, "*Role of Bioinformatics In Biotechnology Concerning AI*", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.6, Issue 2, Page No pp.8-17, June 2019, Available at : http://www.ijrar.org/IJRAR19K9397.pdf

[18] Sreenivasa Rao Veeranki, Manish Varshney,"*Bioinformatics and Data Science in Medical Research*", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.6, Issue 1, page no.204-214, January-2019, Available :http://www.jetir.org/papers/JETIR1901G29.pdf

[19] Sreenivasa Rao Veeranki, "Metagenomics and Single-Cell Technologies for Microbiome Big-Data Mining: Precision Medicine in the Making" , International Journal of Mechanical Engineering, https://kalaharijournals.com/journals.php,ISSN: 0974-5823 Vol. 7 (Special Issue, Jan.-Mar. 2022)

[20] Sreenivasa Rao Veeranki and Manish Varshney, "Intelligent Techniques and Comparative Performance Analysis of Liver Disease Prediction", International Journal of Mechanical Engineering , https://kalaharijournals.com/ijme-vol7-issue-jan2022part2.php , ISSN: 0974-5823 Vol. 7 No. 1 January, 2022,

[21] Sreenivasa Rao Veeranki, "Bioinformatics and Data Science in Industrial Microbiome Applications: A Review", ISSN: 0974-5823 Vol. 7 (Special Issue 5, April-May 2022) International Journal of Mechanical Engineering, https://kalaharijournals.com/journals.php

[22] Sreenivasa Rao Veeranki, Manish Varshney,"Bioinformatics and Data Science in Medical Research", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.6, Issue 1, page no.204-214, January-2019, Available :http://www.jetir.org/papers/JETIR1901G29.pdf

[23] Sreenivasa Rao Veeranki, "Revolutionary Transform of Supply Chain Design & Management Using Artificial Intelligence and Bigdata Analytics" , International Conference on Recent Development in Engineering Sciences, Humanities and Management, ISBN : 978-81-943584-9-7, 24th-25th January 2020

[24] Sreenivasa Rao Veeranki, "The Method for Pharma Growth Throughout The Drug Lifecycle With Artificial Intelligence In Life Science, International e-Conference on Innovation and Emerging Trends in Engineering, Science and Management, ISBN: 978-93-91535-38-4, 24th and 25th June 2022