A SURVEY ON COMPARING MACHINE LEARNING ALGORITHMS TO IMPROVE EFFICIENCY OF IPV6 NETWORK

Arsalan M. Zargar

Irfan Nazir

Shahida Kawoosa

Abstract: The limitations of IPv4 as far as one of a kind location age have become clear with the GROWING NUMBER of internet-connected devices. The objective of this venture is to further develop IPv6, which utilizes a 128-bit addressing framework to give an adequate number of addresses to the rising number of gadgets. To work on the adaptability and proficiency of IPv6 tending to, this examination utilizes support learning. The framework can powerfully upgrade IPv6 tends to in light of changing organization and natural conditions thanks to reinforcement learning. The task fabricates a framework to work in an evolving climate. This suggests that a specialist watches out for the organization and adjusts IPv6 addresses depending on the situation. The support learning framework decides these ways of behaving, ensuring With the assistance of the undertaking's intelligent recreation interface, clients may effectively partake in IPv6 address improvement. Reward/punishment charts permit clients to perceive how well the framework is performing and adjusting, which works with understanding and the executives of IPv6 tending to.

Index terms - IPv6, IPv6 address, clustering, classification, reinforcement, machine learning, supervised , unsupervised, NDP.

1. INTRODUCTION

IP version 4 (IPv4) is the ongoing IP model used in the Intranet and Web. Before, IPv4 was made to work with data dividing and correspondence among associations. At the point when new clients are acquainted with the Web, how much IPv4 tends to in Local Web Libraries has previously been depleted. In an equivalent vein, classful tending to's subnetting and supernetting didn't help with settling the location exhaustion issue, which made the directing system seriously testing. Because of the proportional connection between the two contrary conventions, IPv6, the main cutting edge Web convention presently being used, is not generally broadly utilized for business purposes and has not yet been completely evolved and carried out. The cutting edge variant of the Web Convention, or IPv6, is otherwise called a raunchy tending to framework that recognizes gadgets all through the organization so they might be found. To guarantee the usefulness of the web discussion, every PC associated with the web is remarkably recognizable by its IP address. Some

time ago, it was accepted that IPv4's 32-bit tending to technique, which served billions of gadgets, was adequate. Then again, the boundless utilization of cellphones, PCs, the web, and presently Web of Things gadgets shows that more locations were wanted by the worldwide local area. [2,3,4] As found in Figure 1, IPv6 utilizes a 128 cycle tending to technique, or 16 bytes (octet) long, which upholds 2128 particular IP addresses for every single gadget or hub associated with the Web. In IPv4 [14], the Dynamic Host Configuration mechanism (DHCP) is the main location appointing system.
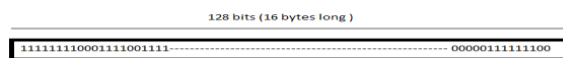

Fig.1 IPv6 address format

Stateful location autoconfiguration and stateless location autoconfiguration are the two location arrangement methods in IPv6. To balance the location exhaustion issue in IPv6, the class honor as in IPv4 is disposed of [6, 7]. Subsequently, factor length blocks are utilized instead of classes in uncouth tending to plans. [14] Four units of one to three digit numbers make up the IPv4 address conspire; eight gatherings of four hexadecimal digits or two bytes long, isolated by a colon, are utilized in IPv6. (:). This is shown in Fig.2

Fig 2 Colon Hexadecimal notation

An IPv6 address may just utilize the zero pressure strategy once. It packs progressive zero divides and replaces them with twofold colons (::). IPv4 and IPv6

blended portrayals [3,4,5,7,8] are likewise allowed utilizing specked decimal and colon hex documentation. The IPv6 documentation will subsequently show up first on the left, trailed by the IPv4 documentation. For IPv6, an objective location can be any of three sorts: unicast, which characterizes a solitary connection point; anycast, which characterizes a gathering of PC frameworks sharing a solitary location; and person, which determines that a solitary gathering part who is by and large reachable gets the parcel. The third sort is known as a multicast address, which likewise indicates a gathering of PCs. In any case, not at all like an Anycast address, all individuals from the gathering will get the message.

2. LITERATURE SURVEY

Low information transmission proficiency, unreasonable energy utilization, and unfortunate start to finish idleness are a portion of the issues with steering strategies in the Internet of Things (IoTs) [1]. Hence, based on fostering a three-layered and correspondence model, a three-layered heterogeneous Internet of Things routing decision-making mechanism based on cellular address (RDCA) is introduced [8,9]. To begin with, the RDCA decides the information sending approaches for network hubs by utilizing hub normal got signal strength and cell automata. Second, IPv6 tending to and course advancement are finished by the RDCA. Cell address at last decides how the directing dynamic cycle is utilized. As per the reenactment discoveries, the typical start to finish delay is 20 ms, the bundle conveyance part of RDCA is somewhere in the range of 82% and 95%, and the directing utilization proportion is somewhere in the range of 20% and

35%. It improves network trustworthiness as well as ensuring the IoT's correspondence execution file.

Since IPv4 tends to run out before the Internet of Things (IoT) at any point exists, IPv6 [3,4,5,7,8] is regularly used to give IoT nodes a remarkable character. This article presents an investigation of IPv6 address task calculations, an examination of the different parts expected to relegate IPv6 numbers to internet of Things nodes, and a glance at the many kinds of IPv6 addresses. [2] The compositional intricacy of IoT advances, convention stacks, IoT hub limits, renumbering, multihoming, IoT network consolidating, and different issues connected with giving IPv6 locations to IoT hubs are additionally featured in this paper [8, 9]. An intensive examination of current tending to strategies that are sorted utilizing designation tables and geological information is given. The location distribution process, execution on different measurements, the application region, and the advantages and downsides of different tending to frameworks are undeniably canvassed in this study. It additionally frames the opportunities for IoT research from now on.

[3] "New Hybrid Method of IPv6 Addressing in the Internet of Things" is a review that examines how people have for a long time truly needed more command over the things around them. We can now achieve this point thanks to the Internet of Things (IoT). A location is vital for an item to have the option to be recognized and followed when it is connected to the internet. Since there are a great deal of these things and they continue to get more, it is ideal to use a tending to space that can deal with this volume of items. IPv6 is the best arrangement in such

manner. There are a few ways to deal with tending to; the main ones are canvassed in this work. This work presents a mixture tending to conspire that consolidates ONS IP and EPC. With the methodology portrayed in this work, each thing has an unmistakable IPv6 address that is coordinated progressively. This is a simple to-carry out approach that requires no additional equipment. Moreover, this approach is viable with a few EPC guidelines, has a low tending to time, and is truly versatile.

The examination local area has commonly accepted that network surveillance assaults in IPv6 networks are unfeasible because of the colossal measure of work expected to address filter each of the 264 hosts in an IPv6 subnet[4]. Be that as it may, by inspecting a few local IPv6 organizations, new examination has shown the suitability of these attacks. The review reached the resolution that by expecting the organization have tending to procedures during examining, a gifted aggressor could rapidly contract the objective hunt field. Truth be told, this raises greater security issues and makes IPv6 organization more uncertain. [4,5] This article presents a clever way to deal with counter surveillance assaults and depicts the current IPv6 tending to plans. The original philosophy is stood out from different current IPv6 tending to plans and tried against a couple of surveillance assault strategies. As to moderation of surveillance assaults, the trial discoveries approve and confirm the adequacy of the tending to procedure.

One more adaptation of the systems administration convention called IPv6 was made to defeat the weaknesses of the ongoing IPv4 standard. IPv4 just

has a 32-digit convey space, however IPv6 [3,4,5,7,8] has a 128-cycle give space, without including framework layer security and adaptability prerequisites. The fundamental issue is that there are immediate contradictions somewhere in the range of IPv4 and IPv6. Plans and structures that stick to one standard can't speak with those that adhere to another, as well as having various lines. [5] With practically zero participation between the two, the query issue of the IPv6 shift permits clients to support their hosts to IPv6 and framework executives to send IPv6 in switches. Since the change from IPv4 to IPv6 can't work out more or less by accident, it should depend on address interpretation advances to empower correspondence across IPv4/IPv6 networks meanwhile. Various query issue adjustment apparatuses have been created to deal with IPv4 and IPv6 framework and structure similarity. In any case, none of the current gadgets handle crucial issues, for example, the non-meddlesome transformation of heritage IPv4-only structures to IPv6 and the working of IPv4-only systems on IPv6-simply focus frameworks. This paper presents an answer for different IP query issues. To tackle the IPv6 address query issue, this article presents a location prefix coordinating directing procedure that might be utilized with both IPv4 and IPv6 PCs. The recommended approach brings down inertness and upgrades address query execution.

3. METHODOLOGY

i) Proposed Work:

The recommended approach utilizes support figuring out how to further develop IPV6 network execution [26]. It utilizes a wise specialist that consistently

watches out for IPV6 address creation and acts proactively to allot new addresses in case of cyberattacks or execution issues. This technique is upheld by a prize punishment framework that urges the Specialist to pick the best strategy, ensuring adaptability progressively and improving organization security and execution. Eventually, the recommended approach furnishes a versatile method for managing issues and raise the overall adequacy of IPV6 network organization. The recommended arrangement powerfully changes IPV6 addressing because of current organization conditions by utilizing Support Learning. This makes it workable for the organization to adjust rapidly to changes, ensuring max execution even despite cyberattacks or spikes in network traffic. By getting rid of manual IPV6 address task, time is saved and human blunder risk is diminished. The framework's capacity to pursue choices all alone really doles out addresses to gadgets, expanding functional viability. The quick development of IPV6 organizations might be really overseen by the proposed arrangement [26]. It can rapidly deal with a rising number of hubs and gadgets, ensuring that address tasks stay aware of the extension of the organization. The framework further develops IPV6 address portions utilizing Support Realizing, which brings down the chance of contentions, inefficient use, and execution issues. Better location the board and more consistent organization activities are the results of this.

ii) System Architecture:

Utilizing a reproduction program, we will initially characterize IPv6 [3,4,5,7,8] addresses in our organization. The addresses will then be practically

distributed to the hubs utilizing an ML strategy (Support). Proficiency of this tending to will be assessed, and once again tending to will be vital on the off chance that effectiveness falls under a foreordained level. Until the ideal degree of effectiveness is reached, the cycle will proceed. Execution will be followed when simply the virtual addressing has been apportioned to the genuine organization. Should there be a decrease in execution, the organization will re-address.
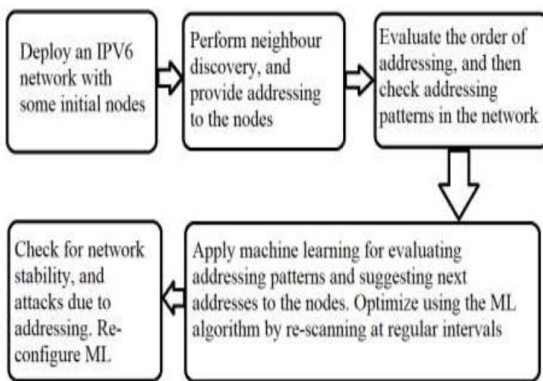

Fig 3 Proposed architecture

In the ongoing organization tending to situation, grouping and characterization strategies are utilized to work with IPv6 tending to. In huge scope establishments, this strategy probably won't find success and could additionally extend the time it takes to give locations to more current nodes. We frequently propose using a reinforcement learning component to decrease inertness and upgrade the result of the tending to plan, or we will consolidate the benefits of a few ML calculations to make another IPv6 tending to plot [2,3,4]. This approach is supposed to work on the general adequacy of IPV6 tending to for little, medium, and huge organizations by further developing the standard tending to quality

through the dissemination of addresses that are for the most part founded exclusively on earlier learning.

iii) Processing:

The accompanying stages make up Fig. 3's recommended plan:

Phase 1: Utilizing a recreation program, this step would initially develop a couple of test nodes to make an IPv6 network utilizing the IPv6 tending to system.

Phase 2: A strategy that should be depicted for settling a bunch of issues connected with the communication between the Nodes connected on a similar connection is expected to address an assortment of issues as follows: stateless autoconfiguration, copy address location, neighbor inaccessibility recognition, address goal, switch revelation, prefix disclosure, and boundary revelation. To perform neighbor revelation, switch requesting, switch notice, and divert messages, this part utilizes the IPv6 Neighbor Discovery Protocol (NDP).

Phase 3: Utilizing a scope of IPv6 address portrayal methods, the example of addressing is confirmed inside the organization to decide the request for 128-cycle IPv6 addresses for identifiers or an assortment of identifiers.

Phase 4: This work utilizes an algorithmic support ML technique to consider the location design ahead of time for the resulting nodes, after stage 3. That is, the addressing will be basically designated to the hubs utilizing an ML strategy. Thus, this step would

decide to utilize Machine learning(ML) strategies to further develop the IPv6 address.

Phase 5: Assuming any bizarre usefulness is found, this stage will change the expected ML calculation and confirm that the organization is steady and free from tending to related attacks.

vi) Modules:

Clients might pick the number of nodes (gadgets) in the IPv6 network they wish to imitate utilizing this application. It lays out the organization's size and intricacy. To recognize it inside the organization, every node is given an extraordinary distinguishing proof number. This works with node the board and following. Inside the reenacted network, the framework creates and instates the foreordained number of nodes. A particular hub ID is doled out to each node. The venture's major thought is this. It relegates and enhances IPv6 locations to nodes progressively involving procedures for reinforcement learning. In light of organization conditions, a specialist makes new IPv6 addresses by persistently checking the organization climate [3,4,5,7,8]. The tending to process is worked on by the utilization of remunerations and authorizations. It presents the reinforcement learning framework's presentation graphically. The advantages and punishments gathered all through the location task method are plotted on a diagram. This helps clients in understanding the adequacy with which the organization's IPv6 addresses are overseen by the framework.
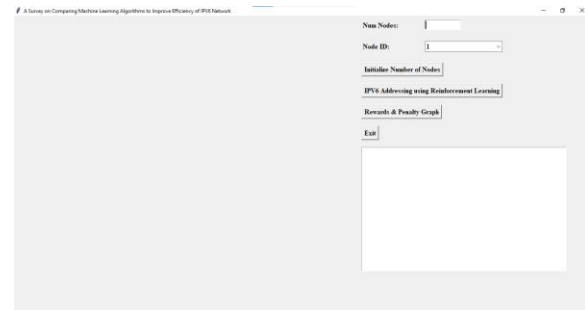
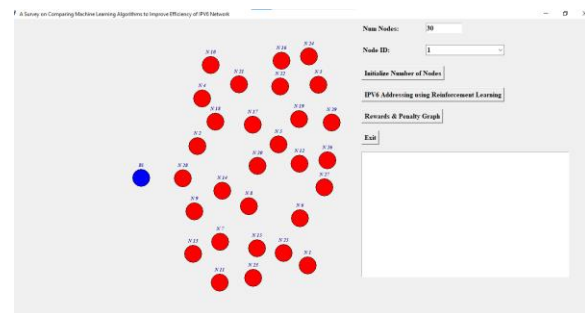**4. EXPERIMENTAL RESULTS**

Fig 4 Home screen
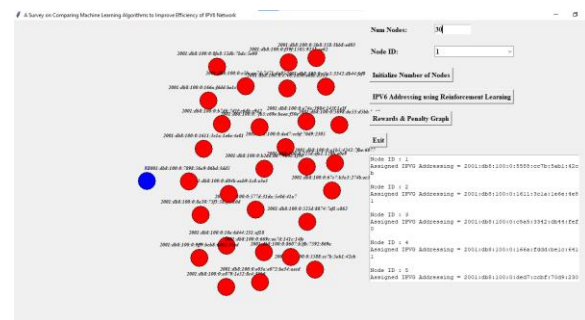

Fig 5 Initialize number of nodes

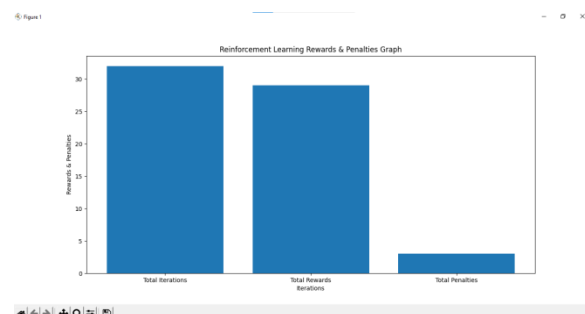Fig 6 IPV6 addressing using Reinforcement learning

Fig 7 Rewards & penalty graph

5. CONCLUSION

The objective of the task is to appropriately deal with the rising number of web associated gadgets by beating the inborn requirements of the IPv4 tending to framework and using the capacity of IPv6's 128-bit tending to conspire. The task gives constant flexibility and thinking abilities to the IPv6 [3,4,5,7,8] network by integrating Reinforcement Learning. These abilities are basic for responding to security dangers and dynamic changes while keeping up with ideal organization execution. Clients might play a functioning job in IPv6 address enhancement on account of the intuitive reproduction interface. IPv6 organization is made simpler with this development, which likewise further develops client commitment by utilizing reward/punishment charts to show framework execution. By settling the downsides of customary tending to and ML methods in IPv6 organizations, the undertaking gives an additional viable and versatile substitute. Support learning is incorporated, which increments productivity as well as ensures security and adaptability in certifiable settings. This task shows guarantee for altering IPv6 network organization because of its inventive methodology and value. It makes the way for more unique and productive tending to arrangements that can meet the always growing requirements of the web associated world.

6. FUTURE SCOPE

By refining classification calculations, further review can further develop IPv6 network interruption recognition frameworks. The fundamental objective ought to be to further develop assault discovery adequacy by utilizing refined include choice techniques and boundary change. In the field of systems administration and disseminated figuring, there is space to examine novel ML ways to deal with make imaginative structures and calculations for future exploration patterns in systems administration, estimation, planning, and expectation. Improving fake brain organizations' preparation terms and adequacy in useful applications, like traffic and log examination, IPv6 IDS sensors, and cyberattack protection, may be the focal point of future review. It is feasible to improve and apply the recommended technique for diminishing IPv6 [3,4,5,7,8] address tasks in useful settings. This will increase current standards for address designations and lift IPv6 tending to's general viability across a scope of organization sizes. Future exploration tries might research the utilization of AI strategies to supervise and upgrading IPv6interface identifier (IID) address allocations. This might entail using artificial neural networks (ANNs) or naïve Bayesian classifiers (NBC) as supported machine learning procedures to tackle IID-related issues [22].

REFERENCES

[1] Ye Tian, Ruixin Miao,i Chen ijun Wang, "Heterogeneous IoTs Routing Strategy Based on Cellular Address," in IEEE International Conference on Smart Internet of ngs, 2018, pp. 64-69.

[2] Kumar Gyanendra, "A Survey of IPv6 Addressing Schemes for Internet of Things," International Journal Hyperconnectivity and the Internet of Things, vol. 2, no. 2, December 2018.

[3] Hamed Najafi, Mehdi Imani Narin Sadat Zarif, "A New Hybrid Method of IPv6 Addressing in the Internet of Things," in International conference of electrical & computer engineering in Iranian Journals & Conf. proceeding, 2018.

[4] Sultan Qaboos University, Muscat, Oman Shubair A. Abdullah, "SEUI-64, bits an IPv6 addressing strategy to mitigate reconnaissance attacks," Engineering Science and Technology, an International Journal 22, pp. 667-672, 2019.

[5] S. Rukmanidevi M.Hemalatha, "Real time prefix matching based IP lookup and update mechanism for efficient routing in networks," Journal of Ambient Intelligence and Humanized Computing, no. Springer, December 2019.

[6] Mahesh Bundele Ramesh Chand Meena, "A Review on Implementation Issues in IPv6 Network Technology," Internal Journal of Engineering Research and General Science, vol. 3, no. 6, pp. 800-809, Nov-dec 2015.

[7] Rahmat Budiarto, Sureswaran Ramadas Raja KumarMurugesan, "Performance Improvement of IPv6 Packet Transmission through Address Resolution Using Direct Mapping," IEEE, 2008.

[8] Paula Herber Benjamin Feldner, "A Qualitative Evaluation of IPv6 for the Industrial Internet of Things," Elsevier, pp. 377-384, 2018.

[9] Ilsun You, Changqia Xu, Honke and Zhang Jianfeng Guan, "The PMIPv6- Based Group Binding Update for IoT Devices," Mobile Information Systems by Hindawi Publishing Corporation, p. 8, 2016.

[10] Normand Belanger, J.M. Pierre Langlois Member IEEE and Yvon Savaria Fellow IEEE Thibaut Stimpfling, "SHIP: A Scalable High-performance IPv6 Lookup Algorithm that Exploits Prefix Characteristics," IEEE, 2017.

[11] Ruba Suliman M. Alowaid and Jin-Ghoo Choi Moneeb Gohar Hind Ahmed M. Alrubaish, "Distributed Group- Based Mobility Management scheme in Wireless Body Area Networks," Hindawi Wireless Communication and Mobile Computing, p. 11 pages, 2017.

[12] D.A. Moskvin, T.D. Ovasapyan D.V. Ivanov, "Approaches to Detecting Active Network Nodes in IPv6 Address Space," Automatic Control and Computer Sciences, vol. 51, no. 8, pp. 902-906, 2017.

[13] Yeong-Sheng Chen and Shang-Yi Liao, "A Framework for Supporting Application Level Interoperability between IP4 and IPv6," Advances in Intelligent Information Hiding and Multimedia Signal processing , Smart Innovation, , System and Technologies, vol. 3, no. 3, pp. 271-278, Oct 2017.

[14] Cheng Yen Wu, Wen Yen Lin, Ta Te Lu, "Comparison of IPv4-over-IPv6 (4over6) and Dual Stack Technologies in Dynamic Configuration for IPv4v6 Address," Advances in Intelligent Information Hiding and Multimedia Signal Processing, Smart innovation , System and Technologies, pp. 259-269, 2017.

[15] Chih-Hsueh Lin, Jia-Long Hu,Chun Liang Chang and Wen Yen Lin Hui-Kai Su, "Design and Implementation of an IPv4/IPv6 DualStack Automatic Service Discovery Mechanism for an Access Control System," Advances in Intelligent Information Hiding and Multimedia Signal Processing, Smart Innovation, Systems and Technologies, pp. 279-284, 2017.

[16] JozefWozniak , Krzysztof Nowicki Tomasz Mrugalski, "Dynamic host configuration protocol for IPv6 improvements for mobile nodes," telecommunication Systems, pp. 1021-1031, 2013.

[17] Lin HE & Gang REN Ying LIU, "GAGMS: a requirement-driven general address generation and management system," Science China Press and Springer-Verlag GmbH Germany, part of Springer Nature 2018, vol. 61, 2018.

[18] ROSILAH HASSAN, AND NOR EFFENDY OTHMAN AMJED SID AHMED MOHAMED SID AHMED, "IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey," IEEE Access, vol. 5, pp. 18187-18210, August 2017.

[19] Senior Member, IEEE, Shu-Wei Qiu, Kai-Kai Chi, Member, IEEE,and Yuguang Michael Fang, Fellow, IEEE Yi-Hua Zhu, "Latency Aware IPv6 Packet Delivery Scheme over IEEE 802.15.4 based Battery-Free Wireless Sensor Networks," IEEE Transactions on Mobile Computing, vol. 14, no. 8, pp. 1-14, 2016.

[20] Ali El Ksimi and Cherkaoui Leghris, "Towards a New Algorithm to Optimize IPv6 Neighbor

Discovery Security for Small Objects Networks," Security and Communciation Networks, vol. 18, no. Article ID 1816462, p. 11 pages, 2018.

[21] John Heidemann Kensuke Fukuda, "Who Knocks at the IPv6 Door? Detecting IPv6 Scanning," in Internet Measurement Conference, Boston, USA, 2018, p. 7 pages.

[22] Mike Johnstine, Andrew J. Woodward Cliton Carpene, "The Effectiveness of classification algorithms on IPv6 IID construction," International Journal of Autonomous and Adaptive Communications Systems, vol. 10, January 2017.

[23] Bahari Belaton, Mohammed Anbar, Basim Alabsi and Ahmed K. Al-Ani Omar E. Elejla, "Comparison of Classification Algorithms on ICMPv6-Based DDoS Attacks Detection," in 5th ICCST 2018, Kota Kinabalu, Malaysia, January 2019, pp. 347-357.

[24] Yong Cui, Xin Wang, Shihan Xiao, and Junchen Jiang Mowei Wang, "Machine Learning for Networking: Workflow, Advances and Opportunities," IEEE Network, pp. 1-8, 2017.

[25] Xiaoqi Ma,Evtim Peytchev Abdulrahman Salih, "Detection and Classification of Covert Channels in IPv6 Using Enhanced Machine Learning," in Proc. of The International Conference on Computer Technology and Information Systems, 2015.

[26] Nikhil Aggarwal, S. Venkatesan Bhanu Vrat, "Anomaly Detection in IPv4 and IPv6 Networks Using Machine Learning," in IEEE INDICON 2015, 2015

[27] Quirin Scheitle, Pawel Foremski, Qasim Lone, Maciej Korczyński, Stephen D. Strowes, Luuk Hendriks, Oliver Gasser, "Clusters in the Expanse:, Understanding and Unbiasing IPv6 Hitlists," in Internet Measurement Conference (IMC '18),Boston, MA, USA. ACM, New York, NY, USA, 2018, p. 15 pages.

[28] Nalinakshi B. G, Dr.D Jayaramaiah Triveni Pujari, "Flow-Based Network Traffic Classification Using Clustering Technique with MLA Approach," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 5, pp. 1855-1862, July 2017.