International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A DDoS Attack Detection Using Deep Learning - A Review

Kunal Kumar[1], Prof Atul Barver[2]

[1] M.Tech CSE, Oriental Institute of Science and Technology, Bhopal (RGPV),
[2] Associate Professor, Oriental Institute of Science and Technology, Bhopal (RGPV)

Abstract:
In this review article, the distributed denial of service (DDoS) assaults are the main topic since they offer a substantial danger to systems linked to the internet and can cause large losses in terms of money, bandwidth and downtime. In this review paper discuss the detection approaches, which are used in traditional methods for identifying and mitigating these assaults, have a limited capacity to identify fresh and changing attack patterns. In this review paper, we provide a deep learning-based DDoS assault detection method. Also discuss the different methods presented by different researchers in the last decade for detection of DoS attack in network.

Keywords: Software Define Network (SDN), Distributed Denial of Services (DDoS), Machine Learning and MATLAB.

I. INTRODUCTION

Attackers that utilize DDoS (Distributed Denial of Service) techniques try to overwhelm a server, website, or network with traffic or requests to ensure that approved individuals cannot access information. DDoS assaults may have a significant negative impact on enterprises, leading to downtime, lost income, and reputational harm [10].

It can be difficult to tell attacker-generated traffic from legal traffic, making DDoS attacks harder to detect. However, there are a number of methods that may be used to identify and stop DDoS assaults, including as [11-14]:

- **Network traffic analysis:** This entails keeping an eye on network traffic for any unusual patterns that could point to a DDoS assault. This may be accomplished via network surveillance instruments and intrusion detection systems (IDS).
- **Anomaly detection:** To do this, algorithms based on machine learning are used to find behavioral patterns that deviate from those found in regular traffic. This may be accomplished by checking for unusual traffic patterns in traffic log analyses.
- **Rate limiting:** To do this, algorithms based on machine learning are used to find behavioral patterns that deviate from those found in regular traffic. This may be accomplished by checking for unusual patterns of traffic in traffic log analyses.
- **Blacklisting:** This involves blocking traffic from known sources of DDoS attacks. This can be done by maintaining a blacklist of known malicious IP addresses or by using a service that provides real-time threat intelligence.
- **Cloud-based DDoS protection:** This involves using a cloud-based service that provides DDoS

protection. These services can analyze traffic in real-time and automatically block traffic from sources that are identified as malicious.

Overall, detecting and mitigating DDoS attacks requires a combination of techniques and technologies. To reduce the impact of these assaults, a thorough DDoS security plan must be implemented.

DDoS (Distributed Denial of Service) DDoS attacks on a server, website, or network are identified and mitigated through the process of recognizing an attack. By detecting and blocking malicious traffic before it reaches the target, detection of DDoS attacks aims to stop or reduce the impact of the assault [15].

DDoS assaults are conducted by a team of assailants or a network of bots, which is a collection of infected machines. These attacks can be challenging to identify and stop since the attacker's traffic is sometimes impossible to differentiate from legal traffic [18].

DDoS assaults may be detected and mitigated using a variety of methods and tools, including network traffic analysis, identification of anomalies, rate restriction, getting placed on a whitelist and based on the cloud DDoS protection. These methods include keeping an eye out for unusual patterns in network traffic, spotting behavior patterns that are not typical of regular traffic, limiting the quantity of traffic that can be sent to a server or network, obstructing traffic from known DDoS attack resources, and using a cloud-based service that offers protection against DDoS attacks [16] [17].

In order to identify DDoS attacks effectively, a complete approach combining various methods and tools is needed. Organizations may lessen the effects of DDoS attacks and guarantee the safety and accessibility of their online services and websites by spotting and countering these assaults.

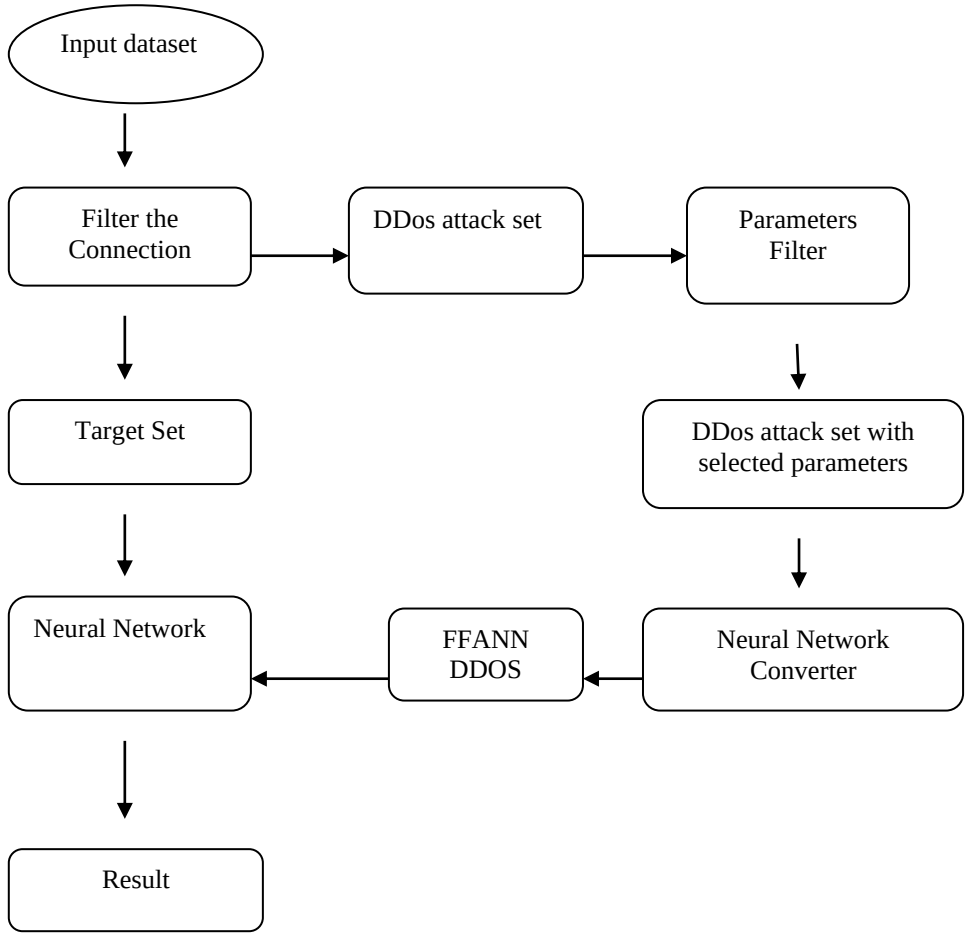

Fig.1 DDoS Attack Detection

I.1 D-DoS Attack and SDN

Distributed denial-of-service (DDoS) attacks have been a real threat for network, digital, and cyber infrastructure .These attacks are capable to cause massive disruption in any information communication technology (ICT) infrastructure. There could be numerous reasons for launching DDoS attacks [18]. These include financial gains, political gains, and disruption. DDoS attacks can paralyse networks and services by overwhelming servers, network links, and network devices (routers, switches, etc.) with illegitimate traffic. They can either cause degradation of service or a complete denial of service resulting in huge losses. Increasing reliance on Internet and data centres has aggravated this problem. Effective solutions for security against DDoS assaults are now required due to the rising reliance of a nation's vital infrastructure on ICT. For instance, in order to continue providing very dependable services, data centres hosting important services, like the smart grid, needs to be safeguarded [19].

For the identification and prevention of DDoS attacks, a variety of proprietary and open-source solutions are available. On the other hand, these attacks are becoming more frequent, sophisticated, and severe. Attackers continue to employ cutting-edge methods to conduct DDoS assaults, making rapid identification and mitigation of these attacks extremely difficult. DDoS attack detection, mitigation, and prevention are now of the utmost importance because of the rising frequency of DDoS assaults and the expanding diversity of their varieties, which are having terrible effects. For instance, one of the top providers of DDoS threat prevention systems, Arbour Networks Inc., reportedly recorded a 334 Gbps assault against a network operator in Asia. Additionally, in 2015 [20], it recorded many assaults with a bandwidth of more than 100 Gbps. numerous cases of this nature clearly demonstrate the necessity for fresh strategies to deal with the DDoS assault issue. The performance and scalability needs of contemporary data centres must be met, and these new strategies must be built to offer the highest levels of security against sophisticated, elusive, and evolving assaults [21-24].

1.2 Software Define Network (SDN)

Many academics have been actively interested in creating SDN-based network security solutions in light of recent developments in software-defined networking (SDN) and its quick and widespread acceptance in the network world. SDN-based approaches have gained increasing attention since being implemented in large-scale wide area networks. Through the SDN controller, the technology enables programmers to centrally manage, programme, and control network assets directly. Routing, policy-based network settings and other persistent networking issues may be solved in unique ways thanks to SDN. While substantial literature is available regarding the security of SDN infrastructure itself, security of SDN-based networks has been a topic of controversy. However, offers an overview of SDN-based DDoS attack detection and mitigation technologies [25] and adopts a favourable stance towards SDN-based security. We discovered that there are several methods for SDN-based detection of DDoS attacks throughout our analysis of the available SDN-based solutions. Based on this research, we classified the current methodologies according to how they identify anomalies. We also pointed out the necessity for an effective DDoS prevention system that can be adjusted to meet the needs of different applications [27].

1.3 DDoS

The goal of a DDoS (Distributed Denial of Service) attack is to stop a server, website, or networks from operating normally by flooding it with a lot of traffic or requests. The attack is carried out by a group of

attackers or a bonnet, which is a network of compromised devices that are controlled remotely by the attacker.

DDoS attacks are often used as a means of extortion, blackmail, or sabotage, and they can have serious consequences for businesses, organizations, and individuals. A DDoS assault may result in downtime, lost sales, reputational harm, and in certain circumstances, legal culpability [26].

DDoS assaults can be difficult to identify and mitigate since the attacker's traffic might be hard to tell apart from genuine traffic. Network traffic analysis, detection of anomalies, rate restriction, blacklisting, and cloud-based DDoS protection are a few of the methods and technologies that may be used to identify and mitigate DDoS attacks.

DDoS assaults pose a significant danger to the safety and accessibility of websites and internet services overall. To reduce the effect of DDoS assaults, it is critical for businesses and individuals to have a thorough plan in place for detecting and mitigating them. DDoS attacks, also known as distributed denial of service attacks, aim to render a website or network resource inoperable by saturating it with malicious data [27-30].

II. Literature Survey

***C Murugesh et.al.* (2023) -** In this research work presented, The use of wireless sensor networks (WSNs), a novel technology with enormous potential, is used in critical situations like battles as well as in business applications like habitat monitoring and smart homes, buildings, and traffic surveillance, among others. Security is one of the key issues WSNs are currently having. However, the use of sensor nodes (SNs) from the unsupervised platform makes the networks susceptible to a variety of potential assaults, and the inherent power and memory constraints of SNs make it hard to use standard security measures. The Spotted Hyena Optimizer with Quantum Neural Network for DDoS Attack Characterization (SHOQNN-AC) approach is developed in this paper for the WSN. The main objective of the SHOQNN-AC approach is to accurately identify attacks utilising DDoS across the WSN successful. The SHOQNN-AC method uses a min-max scalar to do data scaling in order to achieve this. The SHOQNN-AC approach uses a QNN classification model to effectively identify DDoS assaults in the network for DDoS attack detection. The SHO algorithm is used for the choice of parameters process in the SHOQNN-AC approach to increase the attack detection effectiveness. The operational validity of the SHOQNN-AC approach is evaluated using a standard WSN-DS sample. The results of the experiment show how the SHOQNN-AC algorithm is superior to other models **[01].**

***Tariq Emad Ali et.al. (2023)* -** In this research work presented, It could be challenging to differentiate between DDoS attacks with different rates and structures and regular traffic. Over the years, several effective ML/DL methods for spotting DDoS attacks are being put forth by different scientists. Unfortunately, the attackers' continual shift in assault strategy greatly limits the utility of these solutions. With each study's pros and weaknesses indicated, the literature has been compiled in line with the recommended taxonomy for DDoS attack detection using ML/DL approaches. Over 99% accuracy rates have been recorded in a large portion of the literature. Because the bulk of this research evaluated and compared their models utilizing offline data analysis, specific performance indicators may differ in real-world or production contexts. Particularly, we point out that comparisons across the results of existing articles are challenging since they often do not use the same DS or assessment procedures **[02].**

Akshat Gaurav et.al. (2022) - This research work presented, Due to the DDoS attack's ease of usage and capacity to completely exhaust the resources of the target system, cyber criminals frequently employ it. The victim's system is intended to be brought to a complete stop or have its processing power exhausted by the DDoS assault. The DDoS assault is harder to identify when a flash crowds is present, which happens when actual people create a lot of bandwidth. Due to this, swiftly and reliably recognizing DDoS assaults has long been a significant research topic. DDoS assaults and flash mobs are so similar that it is virtually impossible to tell them apart. In this context, we describe a method in this paper that, for small and medium-sized business owners, successfully recognizes DDoS attacks and separates them from the flash crowds using entropy and machine learning. Six machine learning methods were trained using the dataset, which was created using the OMNET++ discrete event simulator. The effectiveness of machine learning algorithms is assessed using the accuracy, f1,precision, and recall, score. On the data sets, aware models, like LR, fared better than others in terms of accuracy, including DT, SVM, LR, MNB, RF, and GB**[03].**

Francesco Musumecit et.al. (2022) – In this research work presented, ML-assisted DDoS attack detection Frameworks for application in SDN environment considering Standalone and Correlated DAD architectures. Leveraging the potential of data-plane programmability enabled by P4 language, we evaluated how detection latency is reduced when performing features extraction at P4 switches. To do so, we compared different ML classifiers in terms of accuracy and computational time, and deployed the algorithms in a real-time scenario in which the P4 switch provides different types of data to the ML classifiers, namely, packet mirroring, header mirroring, and P4-metadata extraction. Numerical results show that attack detection can be performed with classification accuracy, precision, recall and F1-score higher than 98% in most cases, and with drastic time reduction, down to less than 200 sis, in case P4 is used for features extraction. As a future work, we plan to investigate attack-type identification by developing multi-class ML classifiers, and implementing attack detection exploiting ML algorithms which leverage historical data, such as Recurrent Neural Networks **[04].**

Mona Alduailij et.al. (2022) - In this research work presented Detecting DDoS attacks is a frequent issue in a distributed setting. It is crucial to identify this assault since it prevents cloud services from being accessible. An assault of this nature can be recognized using a machine learning model. The goal of this work's research is to more effectively identify DDoS attacks. On the CICIDS 2017 and CIC DDoS 2019 datasets, this experiment was run. In trials, several DDoS attack-related files from both datasets were used. By utilizing the MI and RFFI approaches, we choose the characteristics that are the most important. Machine learning methods (RF, GB, WVE, KNN, LR) are fed the chosen features. With 16 features, RF's total prediction accuracy is 0.99993; with 19, it is 0.999977, and this outperforms earlier strategies. It is determined that employing MI and RFFI as choice of features strategies, RF, GB, WVE, KNN, and LR are producing satisfactory results. For the identification of DDoS and other attacks, we may in the future combine wrapper feature selection techniques, such as sequential feature selection, with artificial neural networks **[05].**

Josue Genaro Almaraz-Rivera et.al. (2022) - This research work presented, A cutting-edge database of information for safeguarding IoT networks. By not include artificial information or class weights, the technique suggested corrects the class imbalance issue of the original dataset, resulting in the development

of a unique IDS based on AI models that focuses on DDoS and DoS assaults. With our three distinct feature sets, the suggested IDS gives results without favoring more than one class, maintaining an accuracy percentage of >99%, and using the Decision Tree as its tool. Tree being the outstanding anomaly detection model, while being practical to implement in real-time production settings, with a remarkable time accomplishment for busy days (evaluating more than 1681 flows/s). Additionally, we used the Decision Tree and the Random Forest method to obtain 100% accuracy, precision, recall, and F1 score metrics for different combinations of Normal flows vs the DDoS/DoS algorithms **[06].**

Firooz B. Saghezchi et.al. (2022) **-** This research work presented, Industry 4.0 CPPSs can use ML to identify DDoS assaults. For the purpose of detecting anomalies in network data flows, we exported network traffic traces (PCAP files) from a large-scale semiconductor fabrication plant in the real world and used 11 different semi-supervised, unsupervised, and supervised ML methods. Prescribed neural networks for learning outperformed design-supervised and unconstrained ones, according on the results of the test.DDoS attacks were pinpointed by DT, RF, and K-NN with accuracy ratings of 0.999, 0.999, and 0.001 for recall, precision, and false positive rate. Although their performance dramatically fell when the PCA method was applied (even with 95% variance retention), the two applied unsupervised techniques (K-Means and EM) still shown extremely high performance (Accuracy = 0.95, Recall > 0.9, Precision > 0.9, and FPR 0.09). This is a surprising result since, in contrast to supervised learning, unsupervised instruction does not call for data labelling, a laborious operation that in practice necessitates a great deal of human work and involvement **[07].**

III. TYPE OF DDOS ATTACK

DDoS assaults come in a wide variety, and attackers sometimes combine more than one form to wreak havoc on their targets. Volumetric, protocol, and application-layer assaults are three important categories [08]. All attacks aim to significantly impede or prevent legal traffic from reaching its destination [31–32]. This can entail prohibiting a user from visiting a website, making a purchase, viewing a video, or connecting on social media, for instance. DDoS may also interrupt company operations by degrading performance or blocking access to resources. Employee access to email or online apps may be restricted as a result, which may hinder them from carrying out their regular duties [34].

Let's dissect the many routes that attackers might follow in order to better comprehend how DDoS assaults function. Seven separate layers make up the Open Systems Interconnection (OSI) paradigm, which serves as a layered framework for multiple networking protocols. Similar to the floors of an office block, where distinct business operations are carried out on each level, each layer of the OSI model serves a specific role. Depending on the sort of online or internet-facing asset they want to disrupt, attackers focus on several tiers [35-37].

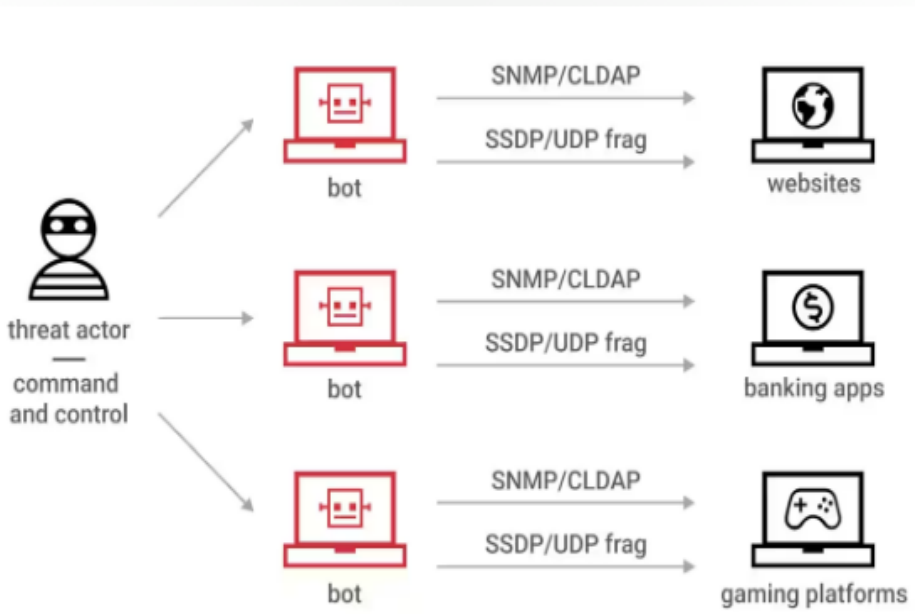

Fig.2 Distributed Denial of Service

A DDoS or DoS attack is comparable, from a high perspective, to an unanticipated traffic bottleneck brought on by a large number of phony ride-share requests. The requests to ride-sharing services seem legitimate, and they send out drivers for pickup, which invariably congests the downtown roadways. This delays the arrival of regular, lawful traffic at its destination [27].

IV. Problem In DDos Attack

DDoS (Distributed Denial of Service) attack detection can provide significant benefits to organizations, there are also some potential disadvantages to consider:

- **Complexity**: DDoS attack detection systems can be complex to implement and maintain, requiring specialized knowledge and expertise. This can add to the cost and time required to deploy and maintain such systems.
- **Resource consumption:** DDoS attack detection systems can consume significant network resources, such as processing power and bandwidth, which can impact overall network performance [35].
- **Limited effectiveness**: Although DDoS attack detection can aid in attack identification and mitigation, it might not be completely successful against all forms of assaults. Attackers may also employ complex strategies to get around detection systems.
- **Cost:** It can be expensive to implement DDoS attack detection, especially for smaller organizations with constrained resources. Some organizations may find the expense of implementing and maintaining these systems exorbitant.
- **Bandwidth saturation:** DDoS attacks flood the targeted system with a massive amount of traffic, causing the system's bandwidth to become saturated. As a result, genuine users may experience delayed or unavailable services.
- **Server overload:** The computing power and memory of the targeted server may be overloaded by DDoS assaults, resulting in a crash or unresponsiveness [37].

- **Application layer attacks:** Some DDoS attacks target specific applications or services running on the server, causing them to become unavailable or perform poorly.
- **Reputation damage:** DDoS attacks can damage the reputation of the targeted system or organization, causing users to lose trust in its services.
- **Financial losses**: DDoS attacks can result in financial losses due to lost revenue, increased operational costs, or the need to invest in additional security measures help stop assaults in the future.

Overall, while DDoS attack detection provides significant benefits for organizations, it is important to consider the potential disadvantages as well, such as false positives, complexity, resource consumption, limited effectiveness, and cost. Organizations should carefully evaluate their specific needs and resources before implementing DDoS attack detection solution

V. Conclusion and Future Work

The review paper primarily describes the DDoS assault and the many DDoS attack types that can happen. DDos is a rapidly expanding issue. It also discusses the many available techniques for detecting DDoS attacks, including packet marking techniques like PPM and DPM, trace back methods, IP trace back divided into proactive and reactive approaches, and entropy variation. Another method that aids in detection is the intrusion detection and prevention system.

Cyber security experts have a perpetual struggle in identifying and preventing DDoS assaults because attackers are always changing their strategies and methods to get around current defenses. Here are some potential future directions for DDoS attack detection:

- **Machine learning and AI-based solutions:** Machine learning and artificial intelligence (AI) technologies can assist in the real-time detection of DDoS assaults by finding patterns and abnormalities in network traffic due to the rising quantity of data created by networks and systems.
- **Block chain-based solutions:** Block chain technology can provide a distributed and decentralized platform for detecting and mitigating DDoS attacks. By creating a network of nodes that work together to detect and filter out malicious traffic, Block chain-based defenses against DDoS assaults can be more reliable and safe.
- **Collaboration and information sharing:** The early identification and prevention of DDoS assaults can be facilitated through cooperation between various organizations and information exchange. Organizations may more effectively prepare for and prevent upcoming attacks by exchanging information about previous assaults and identified harmful sources.
- **Cloud-based solutions:** Cloud-based DDoS detection and mitigation solutions can provide a scalable and flexible defense against DDoS attacks. By leveraging the resources of cloud providers, organizations can quickly scale up their defenses to handle large-scale attacks.
- **IOT-specific solutions**: With the increasing adoption of IOT devices, attackers are targeting these devices to launch DDoS attacks. IOT-specific solutions that can detect and mitigate DDoS attacks on these devices can help prevent these attacks from spreading to the larger network.

REFERENCES

1. C. Murugesh; “Modelling of Optimal Quantum Neural Network for DDoS Attack Classification in Wireless Sensor Networks” 02-04 February 2023.
2. Tariq Emad Ali,Yung-Wey Chong, and Selva kumar Manickam “Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review” Volume 13, Issue 5, 2 March 2023.

3. Akshat Gaurav,Brij B. Gupta and Prabin Kumar Panigrahie "A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs" 2022 Feb 3.
4. Francesco Musumeci, Ali Khan Fidanci, Francesco Paolucci, Filippo Cugini & Massimo Tornatore "Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks" 02 November 2021.
5. Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Alduailijand Fazila Malik "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method" Volume 14 Issue 6, 27 May 2022.
6. Josue Genaro Almaraz-Rivera, Jesus Arturo Perez-Diaz and Jose Antonio Cantoral-Ceballos "Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models" Volume 22 Issue 9, 28 April 2022.
7. Firooz B. Saghezchi, Georgios Mantas, Manuel A. Violas, A. Manuel de Oliveira Duarte and Jonathan Rodriguez "Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs" Volume 11 Issue 4 , 16 February 2022.
8. Samuel Black; Yoohwan Kim "An Overview on Detection and Prevention of Application Layer DDoS Attacks" 04 March 2022.
9. Kanwal Rashid, Kanwal Rashid , Yousaf Saeed, Abid Ali, Faisal Jamil, Reem Alkanhel and Ammar Muthanna "An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs)" Volume 23 , Issue 5, 26 February 2023.
10. M. Dhinu Lal And Ramesh Varadarajan "A Review of Machine Learning Approaches in Synchrophasor Technology" Volume 11, 2023.
11. Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Alduailijand Fazila Malik "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method" Volume 14 Issue 6, 27 May 2022.
12. Josue Genaro Almaraz-Rivera, Jesus Arturo Perez-Diaz and Jose Antonio Cantoral-Ceballos "Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models" Volume 22 Issue 9, 28 April 2022.
13. Firooz B. Saghezchi, Georgios Mantas, Manuel A. Violas, A. Manuel de Oliveira Duarte and Jonathan Rodriguez "Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs" Volume 11 Issue 4 , 16 February 2022.
14. G.C. Amaizu, C.I. Nwakanma, S. Bhardwaj, J.M. Lee, D.S. Ki "Composite and efficient DDoS attack detection framework for B5G networks" Volume 188, 7 April 2021, 107871.
15. Xiang Yu, Wenchao Yu, Li,Xianfei Yang,Ying Chen and Hui Lu "WEB DDoS Attack Detection Method Based on Semi supervised Learning" Volume 2021 , 29 Nov 2021.
16. Mazhar Javed Awan , Umar Farooq, Hafiz Muhammad Aqeel Babar, Awais Yasin, Haitham Nobanee , Muzammil Hussain , Owais Hakeem and Azlan Mohd Zain "Real-Time DDoS Attack Detection System Using Big Data Approach" Volume 13 Issue 19 , 27 September 2021.
17. Özgür Tonkal, Hüseyin Polat, Erdal Ba¸saran, Zafer Cömert and Ramazan Kocao ˘glu "Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking" Volume 10 Issue 11, 21 May 2021.
18. Yadav, Pranay, Bharat Bhushan Khare, Sudesh Gupta, Yash Kumar Kshirsagar, and Swati Jain. "Multi-Band Rectangular Zig-Zag-Shaped Microstrip Patch Antenna for Wireless Applications."

In Design and Optimization of Sensors and Antennas for Wearable Devices: Emerging Research and Opportunities, pp. 66-86. IGI Global, 2020.

19. Yadav, Pranay, Shachi Sharma, Prayag Tiwari, Nilanjan Dey, Amira S. Ashour, and Gia Nhu Nguyen. "A Modified Hybrid Structure for Next Generation Super High Speed Communication Using TDLTE and Wi-Max." In *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, pp. 525-549. Springer, Cham, 2018.
20. Sharma, Bharti, Sachin Kumar, Prayag Tiwari, Pranay Yadav, and Marina I. Nezhurina. "ANN based short-term traffic flow forecasting in undivided two lane highway." *Journal of Big Data* 5, no. 1 (2018): 1-16.
21. Yadav, Ashok, Vinod Kumar Singh, Pranay Yadav, Amit Kumar Beliya, Akash Kumar Bhoi, and Paolo Barsocchi. "Design of circularly polarized triple-band wearable textile antenna with safe low SAR for human health." *Electronics 9*, no. 9 (2020): 1366. (SCI-E).
22. Arvind kumar Singh, Shailesh Kumar Prajapati, Prem Chandra Yadava , Pranay Yadav,"A Performance Analysis of Modified LDPC Based CP-OFDM IDMA on Different Window Size FFT for Next Generation Communication System", Neuro Quantology (ISSN 1303-5150), Scopus Q2 (2022). (Accepted)
23. Munesh Sangwan, Dr. Gopal Panda, Pranay Yadav, "A Comprehensive Analysis of Different MIMO Antenna for Enhancement Performance Using Various Parasitic Elements", Neuro Quantology (ISSN 1303-5150), Scopus Q2 (2022). (Accepted)
24. Yadav, Pranay, Nishant Chaurasia, Kamal Kumar Gola, Vijay Bhasker Semwan, Rakesh Gomasta, and Shivendra Dubey. "A Robust Secure Access Entrance Method Based on Multi Model Biometric Credentials Iris and Finger Print." In Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021, pp. 315-331. Singapore: Springer Nature Singapore, 2023.
25. Kumar, Alok, Sandeep Kumar Shukla, Archana Sharma, and Pranay Yadav. "A Robust Approach for Image Super-Resolution using Modified Very Deep Convolution Networks."*In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pp. 259-265. IEEE, 2022.
26. Mishra, Akhil, Ritu Shrivastava, and Pranay Yadav."A Modified Cascaded Feed Froward Neural Network Distributed Denial of Service Attack Detection using Improved Regression based Machine Leaning Approach."*In 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 1292-1299. IEEE, 2022.
27. Tiwari, Sandeep, Nitesh Gupta, and Pranay Yadav. "Diabetes Type2 Patient Detection Using LASSO Based CFFNN Machine Learning Approach."*In 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 602-608. IEEE, 2021.
28. Tiwary, Abhigyan, M. Kumar, and Pranay Yadav."Prediction of Covid-19 Patient in United States of America Using Prophet Model." In *2021 International Conference on Advances in Technology, Management & Education (ICATME)*, pp. 94-99. IEEE, 2021.
29. Tiwari, Prayag, Pranay Yadav, Sachin Kumar, Brojo Kishore Mishra, Gia Nhu Nguyen, Sarada Prasad Gochhayat, Jagendra Singhk, and Mukesh Prasad. "Sentiment analysis for airlines services based on Twitter dataset." *Social Network Analytics: Computational Research Methods and Techniques* 149 (2018).
30. Singh, Jagendra, Mukesh Prasad, Yousef Awwad Daraghmi, Prayag Tiwari, Pranay Yadav, Neha Bharill, Mahardhika Pratama, and Amit Saxena. "Fuzzy logic hybrid model with semantic filtering

approach for pseudo relevance feedback-based query expansion." In 2017 *IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1-7. Ieee, 2017.

31. Chavate, Shrikant, Ravi Mishra, and Pranay Yadav. "A Comparative Analysis of Video Shot Boundary Detection using Different Approaches." In *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp. 1-7. IEEE, 2021.
32. Yadav, Pranay. "Color image noise removal by modified adaptive threshold median filter for RVIN." In 2015 *International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV)*, pp. 175-180. IEEE, 2015.
33. Sharma, Shachi, and Pranay Yadav. "Removal of fixed valued impulse noise by improved Trimmed Mean Median filter." In *2014 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-8. IEEE, 2014.
34. Yadav, Pranay, and Parool Singh. "Color impulse noise removal by modified alpha trimmed median mean filter for FVIN." In 2014 *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-8. IEEE, 2014.
35. Gupta, Vikas, Dilip Kumar Gandhi, and Pranay Yadav."Removal of fixed value impulse noise using improved mean filter for image enhancement."*In 2013 Nirma University International Conference on Engineering (NUiCONE)*, pp. 1-5. IEEE, 2013.
36. Maurya, Sweta, Shilpi Sharma, and Pranay Yadav."Internet of things based air pollution penetrating system using GSM and GPRS." In *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*, pp. 1-5. IEEE, 2018.
37. Shrivastava, Ritu, Abhigyan Tiwary, and Pranay Yadav. "Challenges Block Chain Technology Using IOT for Improving Personal and Physical Safety-Review."*In 2021 International Conference on Advances in Technology, Management & Education (ICATME)*, pp. 238-243. IEEE, 2021.
38. Yadav, Pranay, Alok Upadhyay, V. B. Prasath, Zakir Ali, and Bharat Bhooshan Khare. "Evolution of Wireless Communications with 3G, 4G, 5G, and Next Generation Technologies in India."*In Advances in Electronics, Communication and Computing, pp. 355-359. Springer*, Singapore, 2021.