IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

NETWORK TRAFFIC ANALYZER

V.Soumya, B.Sneha Durga, Tavanam.Venkata Rao
B.T ECE Student, B.T ECE Student, Associate Professor
Department of Electronics and Communications Engineering
Sreenidhi Institute of Science and Technology, Telangana, India.

Abstract : Due to the quick development of numerous network applications and internet services,the rapid expansion of Internet traffic has become a significant problem.The difficulty for Internet Service Providers(ISPs) is to maintain a certain Quality of Service while optimizing the performance of their neworks in the face of consistently rising IP traffic.Today,it is impossible to imagine living without the internet.In order to spot abnormalities,improve performance and keep a look out for assaults,network availability and activity must be closely monitored.It gathers both historical and real-time data on network activity.It is crucial for keeping track of network availability.Many research have recently been drawn to the analysis and forecasting of network traffic because they have applications across a broad spectrum of industries.To pinpoint numerous issues with current computer network applications,several experiments are carried out and then reported.Network traffic analysis and prediction are proactive measures to guarantee secure,dependable and high-quality network communication.For evaluating network traffic, a variety of methods,from data mining methods to methods based on neural networks,are developed and tested.Several similar linear and non-linear methods for forecasting network traffic are proposed.Several fascinating combination of network analysis and prediction approaches are employed to get effective and profitable results.

IndexTerms **– Internet Service Providers,Quality of Service,IP traffic.**

I. INTRODUCTION

Network traffic is the volume of data travelling from a source to a destination over a network at any given moment. The essential building blocks of network data transfers are packets, which make up the conveyed data. Traffic data is broken into distinct packets during data transfer from the source and afterwards reassembled at the destination. Today, it is impossible to imagine living without the internet. Internet traffic is extremely high as a result of the Internet's rapid growth. Video streaming websites like Netflix and YouTube are responsible for the majority of today's internet traffic. Both the average traffic volume and the predictability of data traffic patterns have increased.

Monitoring and analysing network traffic has therefore become crucial in order to when issues arise, efficiently troubleshoot and fix them to keep network services from being interrupted for an extended period of time. The practise of "traffic monitoring" keeps an eye on network activity and alerts the administrator to any outages. Network administrators have access to a variety of network monitoring tools that employ various monitoring methodologies to track and examine network data. Security for broadband Internet access depends on the adoption of access control lists and the execution of perimeter regulations. These techniques are risky since they are based on generic, infrequently updated profiles that lack information on the hazard posed by residential users. The findings demonstrate that the suggested characterization permits alert classification with a sensitivity of 93% in distinguishing between normal and anomalous flows and permits a 73% reduction in traffic directed at the traffic analyzer, validating the gathered dataset and permitting more adaptable and efficient access network security.

II. NEED OF THE STUDY.

The major goal is to increase the efficiency of their networks in the face of steadily rising IP traffic while ensuring a particular Quality of Service. Today, network traffic analysis is increasingly crucial and significant for keeping track of network traffic. In the past, administrators would only monitor a small number of network devices or a few hundred computers. It's possible that the network bandwidth was only around 100 Mbps (Megabits per second). Currently, network managers must manage wired networks with speeds more than 1Gbps, wireless networks, and ATM (Asynchronous Transfer Mode) networks (Gigabits per second). They require additional modern network traffic analysis tools in order to maintain network security, monitor the network, and quickly address network problems in order to prevent network failure. As a result, network traffic analysis is now plagued by a number of issues. A network is scrutinised for security management on a number of levels, including the packet, flow, and network levels. Researchers use a range of techniques for network traffic analysis. After preprocessing, actual analysis and observation are used to find patterns in the network data as part of a generic framework for network traffic analysis

III. LITERATURE SURVEY

3.1 Network Traffic flow

In today's complex networks, network monitoring and measuring have grown in importance. Formerly, administrators might only keep an eye on a handful.A total of 31 network devices or fewer than 100 computers. Although the network capacity may just be 10 or 100 Mbps (Megabits Per Second), administrators now have to deal with both wireless networks as well as higher speed wired networks (more than 10 Gbps (Gigabits Per Second) and ATM (Asynchronous Transfer Mode) networks). In order to maintain the network system stability and availability, such as to fix network issues quickly or prevent network failure, to assure the network security's robustness, and to make wise network planning decisions, they need more advance)d network traffic monitoring and analysis tools.

Monitoring agents must find, isolate, and fix network issues when a failure occurs, and they may also need to recover thefailure. The administrators should typically be warned by the agents to rectify any issues within a minute. The administrators' duties still include regularly checking for threats coming from the inside or outside of the network despite the reliable network. Also, if the network devices are overloaded, they must frequently verify the network performance.

Information regarding network consumption can be utilized to create a network plan for short- and long-term improvement before a failure due to overload.There are many different types of tools for network monitoring and analysis, including those for Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), sniffing, and network flow analysis. Administrators can comprehend network activity, including application and network usage, resource utilisation, network anomalies, and security flaws, given the data packet and network traffic flow information. In this paper, we review every monitoring and analysis tool for network traffic that is available, in both public and commercial settings.

3.2 Traffic flow

In order to record network traffic flow data and then transmit it back to the monitoring hosts, Cisco Systems offers “Cisco Netflow”, an open but proprietary network protocol that runs on Cisco IOS(Internetworking Operating System).We describe network traffic flow data from Netflow-like devices in this section.The term ‘Netflow-like’, despite the fact that they use different methods to retrieve or export network flow data.For instance, Juniper Networks offers “ cflowd ”,which is essentially Netflow version 5, as a similar capability for its routers.The same ‘NetStream’ technology is also supported by routers made by Huawei Technologies.Tools for network monitoring and analysis are becoming more and more necessary as the network expands. The administrators' responsibilities include not just keeping track of network outages and resolving them quickly, but also preventing network outages caused by network overload or external threats. The administrators' needs are satisfied using the network traffic information. The characteristics of network traffic and network utilisation, for instance, can identify security flaws. Moreover, network planning can be done using the sort of application that uses the bandwidth. In this research, we divided network traffic into three groups: local traffic from packet sniffers, network traffic from SNMP-like devices, and network traffic from NetFlow-like devices.Some well-known paid and free utilities are listed along with details on their functionality and operating system compatibility. These categories have been compared, and depending on what the administrators want, different techniques are used. For instance, SNMP is better suited for remote management and configuration but provides less data that can be used for additional network traffic monitoring.A local tool where the device is attached is called a packet sniffer. Although NetFlow-like data is excellent for further analysis, there are still certain drawbacks, such as expensive implementation and privacy issues.

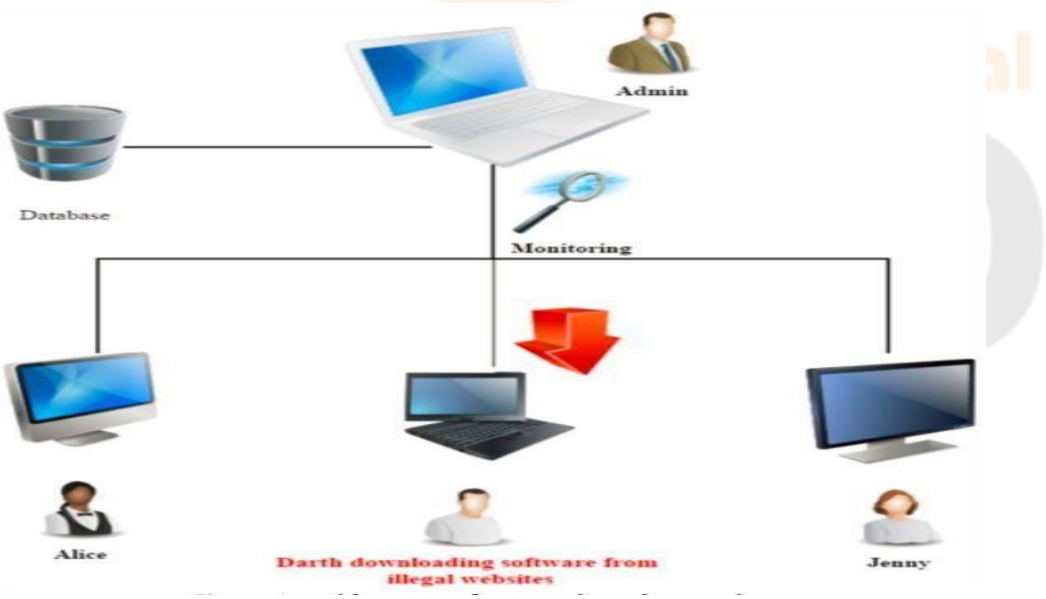

Fig.1.Diagram of Network Traffic Analyzer

IV. NETWORK ANALYSIS TOOLS

Understanding what is really going on on the network, figuring out who is using the most bandwidth, and figuring out whether any behaviour that can result in bandwidth congestion is taking place can be difficult for a network administrator. Every day, numerous operations are carried out on a network to meet organisational objectives. These challenges take several shapes for large corporations and dispersed networks. Network analysis is necessary for IT administrators to have a comprehensive picture of what's happening. You can successfully monitor, inspect, and debug your network using real-time network analysis, which gives you access to information about your network traffic.
Many network data points must be analysed as part of network analysis, including

- Source-specific traffic
- Traveler's destinations
- Protocol-specific traffic
- Application-specific traffic

You need sophisticated network analysis tools that can also gather and analyse network traffic in order to obtain all of the aforementioned data. Without these data points, you won't be able to evaluate the trend in bandwidth use, establish whether each network action is legitimate or an attack, or ensure that your bandwidth is optimised to give business-critical activities

SOFTWARE REQUIREMENTS

The OS is Windows 11. The language is Python of Spyder IDE.
Networkx , matplotlibrary are special tools.

V. WORKING/PROCESS

5.1 Capturing the Network Traffic

In order to assess network traffic for the proposed system, it must first be captured. The Waikato Environment for the Knowledge Analysis (WEKA) programme and the TensorFlow library are used to convert the traffic into a readable format after it has been gathered using the tcp dump tool [64]. To create the dataset, network traffic from a university campus is collected and captured. It is significant to note that three experts classified the assaults into DDoS, Infiltration, Brute Force, and Web attacks after classifying the data used to create the dataset. The experts examine the key elements, including flow quantity, source flow, and address fluctuation.

5.2 Dataset

An essential part of network traffic analysis is testing and evaluation. It is advised to utilise a standard data collection in order to compare the effectiveness of all research projects using a similar standard list. Many common data sets have been employed in recent years. We make advantage of a few significant data sets that are currently being used by researchers to study network traffic.

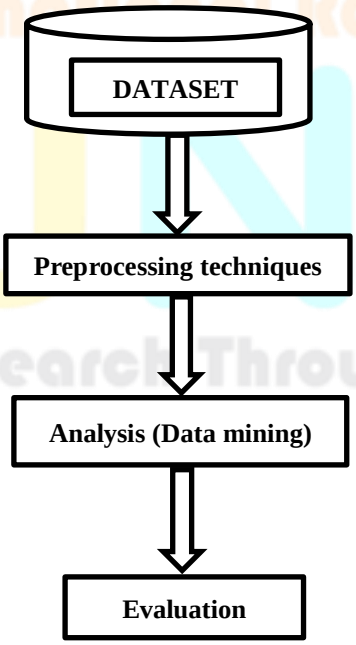

Fig.2. Diagram of Generic structure of network traffic analysis

Data from DARPA The most popular method for assessing network traffic analysis in terms of intrusion detection has been using KDD cup data. Stolfo et al. give this data collection. It is built using information has 24 training and test attacks, plus an additional 14 varieties that are noted in test results. NSL-KDD data set 2. An enhanced version of the KDD cup data set is called the NSL-KDD data set.The NSL-KDD data collection does not contain duplicate entries in testing data or redundant instances in training

data.As a result, the classifier becomes more precise. Researchers can access the NSL-KDD, an enhanced version of the original KDD cup data set, for free.

5.3 Preprocessing Techniques

Preprocessing is a crucial step in the process of transforming real-world data into a format that can be understood. Real-world data have undoubtedly been noisy and frequently incomplete. To put it another way, the vast majority of the real-world data that we want to analyse using data mining techniques is insufficient and inconsistent (containing errors, outlier values). Prior to using data mining techniques, preprocessing techniques are required to enhance the quality of the data. The accuracy and effectiveness of the resulting data mining task are boosted as a result. Network traffic analysis requires the use of preprocessing techniques since network traffic patterns come in a wide variety of formats and dimensionalities. We give in-depth explanations of different techniques used in network traffic analysis in the following subsections.

5.4 Analysis

While examining network traffic, data mining is crucial. Our goal is to provide several data mining methods used by academics to examine network traffic. Data mining approaches have been divided into four main groups, including clustering, classification, hybrid, and association rules techniques.

5.5 Evaluation Metrics

Numerous various metrics are employed in data mining approaches to investigate them. The performance of the classifier is evaluated using the metrics of detection rate, false positive rate, accuracy, and time cost for various data sets. Predictive accuracy can be expressed using a variety of metrics. the measures that make use of a confusion matrix.

VI. RESULTS AND DISCUSSION

Python uses matplotlib for graphical charting ,and we use the utility function def get data(file name) to load data from files. Header is the first element in the list ,and data should start from the first line return header and data .Graph objects are created using network graph . A loop is used to add data to a node, and another for loop is used to add data to an edge. Degree centrality is used to determine the number of nodes connected , and Closeness centrality displays the average distance between nodes and provides the shortest distance between nodes and Betweenness centrality displays how one node influences the others.
This function examines the information that is being transferred from one node to another node using the data from the nodes and edges file. Using the a forementioned functions ,it will assess the whole network and bandwidth range to determine whether it will be adequate for sending information from these nodes .If not ,it will consider it as traffic and draw a graph that displays the traffic between the relevant nodes.

VII. CONCLUSION

This network traffic analysis reveals that the campus network is utilising bandwidth inappropriately, which is a critical and developing concern for practically all organizations in the current information technology environment. Access to the Internet is restricted due to improper bandwidth management, which results in poor-quality academic and research output. Internet connectivity is made more accessible, especially for those who actually need it, thanks to better bandwidth control. Sadly, a lack of technical staff, inadequate implementation of Internet usage policies, a lack of knowledge, a lack of assistance from authorities, etc. have all contributed to a relatively low level of understanding of the significance of controlling bandwidth. Since bandwidth is a scarce and precious resource, it is important to raise awareness among all stakeholders in the university education system,including students,researchers ,staff and to implement a single,accepted policy. Policies should promote academic and research-related activities and discourage pointless and person-centered ones. The ICT specialists in charge of managing the university network system are required to regularly monitor network traffic and user behaviour on the network, followed by a study of online applications consuming precious resources. In addition, offering trainings and technical tools is insufficient for bandwidth management; instead, all stakeholders, the relevant authorities, and ICT employees must work closely together to develop a unified, acceptable Internet access policy.

VIII. ACKNOWLEDGMENT

We wish to express our deep sense of gratitude to our Internal Guide Dr.T.Venkata Rao and Project Coordinator Dr.SN.Chandrashekhar .Dr.T.Venkata Rao ,Associate Professor (ECE) who have taken grate care in the project work undertaken ,by devoting his valuable time in advising and guiding us at each phase , leading to successful completion of our project work. It has been educative and enlightening experience working with him. We are greatly in debited to prof.Dr.S.P.V.SUBBA RAO ,Head of the Department of Electronics and Communication for providing valuable guidance at every stage of this project work. We are thankful to our principal Dr.T.CH.SHIVA REDDY for providing valuable guidance and support at every stage of this project work. We are profoundly grateful to our director Dr. C.V. TOMY and college authorities for helping us in completing our project work. We would also like to thank all our other faculty members and staff who supported us completing the project work.

IX. REFERENCES

[1]. Dualwan (2009) Bandwidth Management and Traffic Optimization (2010). http://dualwan.org/ bandwidth-management.html

[2]. [Cisco, NetFlow06a] Cisco Systems, "Cisco CNS NetFlow Collection Engine". http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/index.html

[3]. [cflowd98] CAIDA, "cflowd: Traffic Flow Analysis Tool". http://www.caida.org/tools/measurement/cflowd/design/design-1.htm

[4]. [flowd06] "Flowd" http://www.mindrot.org/projects/flowd/

[5]. [Wireshark06] "Wireshark". http://www.wireshark.org/

[6]. M Joshi, TH Hadi - arXiv preprint arXiv:1507.05722, 2015 - arxiv.org

[7]. M Abbasi, A Shahraki, A Taherkordi - Computer Communications, 2021 - Elsevier

[8]. https://www.networkstraining.com/network-traffic-analyzer-tools/

[9]. https://www.google.com/amp/s/www.dnsstuff.com/networktrafficanalyzers/amp