NETWORK TRAFFIC ANALYZER

[1]G. Archana, [2]I. Vyshnavi, [3]J. Srighana, [4]E. Lavanya, [5]Dr. Shruthi Bhargava Choubey

[1,2,3] Students, [4]Assistant Professor, [5]Dean Innovation,
Electronics and Communication Engineering
Sreenidhi Institute of Science and Technology (SNIST),
Affiliated to JNTUH, Ghatkesar, Hyderabad.

***Abstract* – Because of the rapid development of numerous network applications and internet services, the rapid expansion of internet traffic has emerged as a key challenge. One of the issues that internet service providers (ISPs) confront is optimizing network performance in the face of ever-increasing IP traffic while maintaining a certain level of quality of service. We can no longer imagine life without the internet. Network traffic analysis is critical for monitoring network availability and activity in order to detect abnormalities, optimize performance, and detect threats. It captures real-time and historical data on what's going on the network. It is critical for monitoring network availability. To pinpoint numerous issues with current computer network applications, various experiments are carried out. A proactive strategy to ensuring safe, dependable, and high-quality network communication is network traffic analysis and prediction.**

Keywords: Network traffic, ISP

I. INTRODUCTION:

The security of broadband Internet access is dependent on the execution of perimeter regulations and the use of access control lists. These techniques are risky since they are based on common and infrequently updated profiles that lack threat information for residential users. The results show that the proposed characterization allows for the classification of alerts with a sensitivity of 93% in the differentiation of legitimate and anomalous flows, as well as a 73% reduction in traffic directed to the traffic analyser, validating the collected dataset and enabling more The volume of data travelling through a network from a source to a destination at any one time is referred to as network traffic. The data is transferred in packets, which are the basic units of network data exchanges. During data transmission, traffic data from the source is broken into individual packets, which are then reassembled at the destination. Today, it is impossible to imagine living without the Internet. The Internet has grown at a rapid pace, resulting in high Internet traffic. Video streaming services like YouTube and Netflix account for the majority of today's internet traffic. The average traffic load has increased, and data flow patterns have become unpredictably erratic. As a result, network traffic monitoring and analysis have become critical in order to properly troubleshoot and repair problems as they arise, so that network services do not stall for extended periods of time. Traffic monitoring is a technology that continuously monitors network traffic and alerts the administrator if there is an outage. There are numerous network monitoring tools available for network administrators that employ various monitoring strategies to monitor and analyse network data. dynamic and efficient access network security.

II. LITERATURE REVIEW

There are several existing models for network traffic analysis, some of which are:

1. Statistical models: These models analyse network traffic by using statistical techniques to identify patterns, anomalies, and trends in the traffic. Examples include time-series analysis, regression analysis, and clustering analysis.
2. Machine learning models: These models use machine learning algorithms to learn patterns in network traffic data and classify it as normal or anomalous. Examples include neural networks, decision trees, and support vector machines.
3. Signature-based models: These models use pre-defined signatures or rules to detect specific types of network traffic, such as malware or network attacks.

Examples include intrusion detection systems (IDS) and intrusion prevention systems (IPS).

4. Behaviour-based models: These models analyse the behaviour of network traffic to identify anomalies and detect potential threats. Examples include anomaly detection systems and threat intelligence platforms.
5. Hybrid models: These models combine different techniques, such as statistical analysis and machine learning, to improve the accuracy of network traffic analysis.

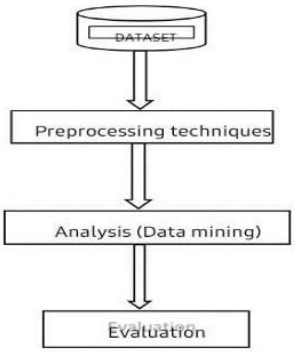
Overall, the choice of model depends on the specific requirements of the network and the nature of the traffic that needs to be analysed.

III. MODELLING & ANALYSIS

To begin, network traffic is recorded and analysed for the proposed system. The tcp dump tool is used to capture traffic, which is then transformed into a readable format via the Waikato Environment for Knowledge Analysis (WEKA) programme and the TensorFlow library [64]. The network traffic is extracted from a university campus and used to build the dataset. It is vital to highlight that the data for the dataset is classified by three specialists, who categorise the attacks as DDoS, Infiltration, Brute Force, and Web attack. The essential aspects, such as flow number, source flow, and address variation, are examined by the experts.

Testing and assessing network traffic is a key part of network traffic analysis. It is recommended to utilise a standard data set to evaluate the effectiveness of all research activities that employ a similar standard list. Several standard data sets have been utilised in recent years. We include a few key data sets that researchers utilise for network traffic analysis.

DARPA data collection KDD cup data has been the most widely used for analysing network traffic in terms of intrusion detection. Stolfo et al. give this data collection. It was built using data from the DARPA IDS evaluation programme. The KDD cup data set has 41 features and roughly 4,900,000 training instances. Furthermore, the test data set includes 300,000 instances. The KDD cup includes 24 training and testing attacks, with an additional 14 varieties reported in test data. 2. Dataset NSL-KDD The NSL-KDD data set has been updated from the KDD cup data collection. The NSL-KDD data collection does not include duplicate entries in testing data or redundant instances in training data. As a result, the classifier becomes more accurate.



Pre-processing is a critical step in transforming real-world data into a comprehensible format. Certainly, real-world data is frequently incomplete and noisy in specific behaviour. In other words, most of the data we want to analyse from the actual world using data mining techniques is insufficient and inconsistent. (containing errors, outlier values). As a result, before applying data mining techniques, pre-processing procedures are required to increase the quality of the data, hence contributing in improving the accuracy and efficiency of the subsequent data mining work. Because network traffic patterns vary in format and dimensions, pre-processing techniques are critical and significant in network traffic analysis. We provide extensive descriptions of these methods in the following subsections.

Data mining is critical in analysing network traffic. Our goal is to demonstrate several data mining techniques used by researchers to analyse network traffic. We divided data mining approaches into four major categories: clustering, classification, hybrid, and association rules.

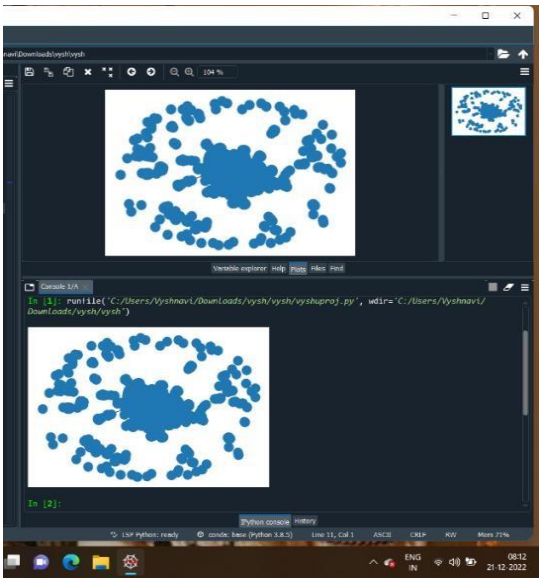
Many different metrics are utilised in data mining approaches to investigate the data mining processes. The detection rate, false positive rate, accuracy, and time cost indicators are used to assess classifier performance for various data sets. There are several metrics for expressing predicted accuracy. The confusion matrix was employed as a metric.

IV. RESULTS & DISCUSSION:

Bottlenecks are likely to emerge as a result of an increase in the number of users in a specific geographic location.

- Trouble shoot bandwidth problems as follows: A slow connection might occur when a network is not equipped to handle an increase in the number of users or activities.
- Improve network device visibility: Greater knowledge of endpoints can assist managers in anticipating network traffic and making required modifications.
- Detect and resolve security concerns more quickly: NTA operates in real time, notifying administrators when there is a traffic anomaly or potential breach.

Network traffic analysis (NTA) is a technique used by network administrators to investigate network behaviour, maintain availability, and detect odd activity. NTA also allows administrators to evaluate whether any security or operational issues exist – or may emerge in the future – under present settings. Taking care of such issues as they arise not only optimises the organisation's resources but also decreases the likelihood of an attack. As a result, NTA is linked to increased security.



V. CONCLUSION:

This network traffic analysis reveals that there is inefficient bandwidth utilisation in the campus network, which is a critical and developing concern for practically all enterprises in today's information technology environment. Inadequate bandwidth management prevents useful Internet access, resulting in low-quality academic and research work. Better bandwidth management expands Internet access, especially for those who need it most. Unfortunately, there is little knowledge of the need of bandwidth management due to a lack of awareness, a lack of technical staff, bad implementation of Internet usage policies, a lack of assistance from authorities, and other factors. Because bandwidth is a very important and finite resource, there is a need to raise awareness among all stakeholders, including students, researchers, and faculty.

Policy should foster academic and research activity while discouraging unproductive and individualistic pursuits [10]. The ICT specialists in charge of managing the university network system must regularly monitor network traffic and user activity on the network, followed by an examination of online applications that consume precious resources. Furthermore, providing training and technological tools is insufficient for bandwidth control; a rich cooperation among all stakeholders, authorities, and ICT personnel on a single acceptable Internet access policy is required. As a result, it is a must to adopt suitable bandwidth control in order to avoid bandwidth hunger in the campus network.

REFERENCES:

1. Dualwan(2009) Bandwidth Management and Traffic Optimization (2010).
2. http://dualwan.org/bandwidthmanagement.html
3. [Cisco, NetFlow06a] Cisco Systems, "Cisco CNS NetFlow Collection Engine". http://www.cisco.com/en/US/products/sw/netm gtsw/ps1964/index.html
4. [cflowd98] CAIDA,"cflowd: Traffic Flow Analysis Tool".
5. http://www.caida.org/tools/measurement/cf lowd/design/design1.html [flowd06] "Flowd"
6. http://www.mindrot.org/projects/flowd/
7. [Wireshark06]"Wireshark" http://www.wireshark.org/
8. M Joshi, TH Hadi - arXiv preprint arXiv:1507.05722, 2015 - arxiv.org
9. M Abbasi, A Shahraki, A Taherkordi - Computer Communications, 2021
10. Elsevier
11. https://www.networkstraining.com/network-traffic-analyzer-tools/