International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 245-254
https://doi.org/10.70917/ijcisim-2026-2508
Article

A Framework for Measuring Network Neutrality Violations in ISP Networks

Archana V. Ugale[1], Meghavarshini S. K.[2], Vikas H.[3], Dr. Sampada Abhijit Dhole[4], Bhavna Talreja[5], Abhijeet Agashe[6]

[1] Department of Information Technology, Sir Visvesvaraya Institute of Technology, Nashik, Savitribai Phule Pune University (SPPU), Maharashtra, India.
Email: archanaugale11@gmail.com
[2]Department of Electronics and Communication Engineering (ECE), Sri Venkateshwara College of Engineering, Bengaluru, Karnataka, India.
Email: meghavarshini.sk_ece@svcengg.edu.in
[3] Department of Electronics and Communication Engineering (ECE), Sri Venkateshwara College of Engineering, Bengaluru, Karnataka, India.
Email: vikas.h_ece@svcengg.edu.in
[4]Department of Electronics and Telecommunication Engineering, Bharati Vidyapeeth College of Engineering for Women, Pune – 411046, Maharashtra, India.
Email: sampada.dhole@bharatividyapeeth.edu
[5]Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India.
Email: bhavna.talreja88@gmail.com
ORCID: 0000-0001-6210-5391
[6]Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India.
Email: agashea@rknec.edu
Scopus Author ID: 36999231500
ORCID: 0000-0002-9434-5565

Abstract: — Network neutrality requires that Internet service providers do not discriminate against any traffic, but the lack of transparency in traffic management ensures that such discrimination is hard to measure and easy to conceal. The paper suggests the use of a multi-faceted approach comprising of active probing, passive monitoring and applications-aware performance measurement as a framework of measuring network neutrality violations in the ISP networks. The framework is meant to detect the discriminative practices, which include throttling, prioritization, blocking, and protocol-specific degradation in heterogeneous access technologies. We design a realistic threat model that also includes the ISP incentives and operation constraints, and derive design requirements that include the focus on accuracy of measurements, scalability, privacy of users, and reproducibility. The suggested architecture unites the concepts of traffic classification, application profiling, and multi-layer QoS and QoE measures to provide the ability to compare fine-grained services, content types, and time intervals. The hybrid measurement methodology is presented and offers a combination of both controlled experiments and large-scale passive flow analysis to enhance coverage and minimize bias. Mechanisms of statistical bias reduction and ground-truth validation are used to separate the areas of deliberate discrimination and performance differences caused by congestion. Empirical evidence has shown that the framework can always identify the presence of unfairness and the existence of performance mismatches in high confidence even when dealing with dynamic networks. The discussion identifies practical deployment, regulatory applicability, and applicability of the encrypted traffic and new transport protocols.

Keywords: — Network neutrality, ISP traffic management, active measurement, passive monitoring, QoS/QoE analysis, fairness evaluation.

1. Introduction

Internet network neutrality is a principle that holds that Internet service providers (ISPs) must not discriminate between different data packets, throttle, prioritize or block them based on content, application, service, or source. This principle has been generally considered as essential to maintaining free Internet, which nurtures innovation, healthy competition, freedom of expression and choice of users. Nonetheless, the growing sophistication in the practice of ISP traffic management, combined with economic pressures to give priority to given services or business partners has brought up consistent worries about the secret undermining of network neutrality. Identifying and establishing such breaches is a major technical and regulatory issue. The current ISP networks are based on advanced tools like traffic forms, deep packet inspection, application-aware scheduling, and dynamic congestion control to optimize the performance and guarantee quality of service. On the one hand, these methods can be considered as legitimate within the current context of network management, on the other hand, however, it provides a loophole to covert and discriminating discrimination that is hard to notice on the side of the end user [1]. Figure 1 depicts combined measurement, analysis, and fair assessment on the detection of ISP neutrality infringement. Besides, the use of encryption, content delivery networks, and dynamic application behaviors are also widely used and can further cloud traffic handling policy visibility.

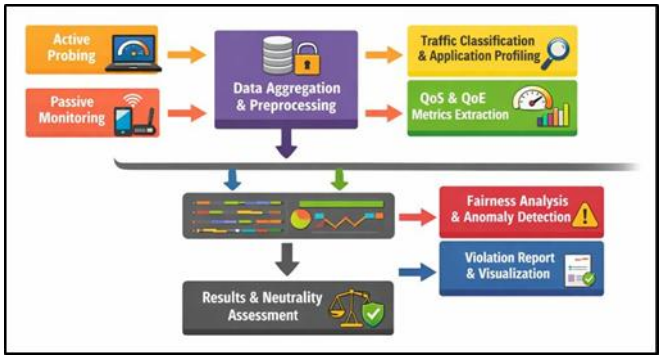

Fig.1. Proposed Framework for Measuring Network Neutrality Violations in ISP Networks

Consequently, the neutrality violations can be in the form of intermittent performance loss, inflation of service-specific latency or unfair bandwidth allocation, which is not easily attributable to innocent congestion effects. The proposals of different measurement approaches to evaluate network neutrality compliance have been made by regulatory bodies and researchers, such as active probing tools, passive traffic monitoring, and crowdsourced performance measurements[2] Despite the contribution of these approaches to the body of knowledge, the current frameworks are usually limited in their scalability, the accuracy of measurements, or measurement bias, or have privacy implications. Most tools are application, protocol-specific, do not have strong ground-truth validation, or are unable to tell intentional discrimination and natural network effects like congestion, routing adjustment, or wireless impairment [3]. As a result, it is apparent that a single, systematic and clear system is needed, which can confidently measure, compare, and derive meaning on network performance, across applications and situations. In this paper, the gap will be filled by suggesting an extensive framework of measuring the violation of network neutrality in the ISP networks. The framework will accommodate both active and passive measurement modalities, which will allow controlled experimentation and a real-world observation of traffic [4].

2. Related Work and Existing Measurement Approaches

A. Active measurement–based techniques

One of the oldest, and most commonly used methods of identifying the violation of network neutrality is active measurement-based techniques. These approaches are based on the creation of controlled traffic patterns by either end hosts or special measurement nodes and monitoring the behavior of the network under specified conditions. Common methods are the so-called packet pair probing, throughput tests, latency measurements, or application-specific traffic replay where the performance of one service or protocol is compared to another [5]. The major benefit of active measurements is that they can be controlled and repeated. Through the use of well planned experimentation, the researcher will be able to isolate the variables and directly test his or her hypotheses concerning discriminatory treatment [6]. Active probing is similarly appropriate to regulatory audits, since it offers reproduced evidence that can be verified on its own. In addition, the techniques can be deployed on-demand, which allows temporal analysis of the

behavior of ISP under changing network conditions. Nonetheless, proactive measures are associated with a number of difficulties. They can create unrealistic patterns of traffic currently unrelated to the actual user behavior, which can result in unusual ISP treatment [7]. Over probing may also create overheads and may lead to ethical or policy issues.

B. Passive Monitoring and Crowdsourced Methods

Crowdsourced measurement and passive monitoring techniques are the approaches that concentrate on monitoring real traffic, instead of introducing artificial probes to the network. Passive methods usually consider flow-level metrics, packet headers or performance aggregates of end hosts, gateways or monitoring points. Such techniques seek to deduce the violation of neutrality by establishing long-term disparities in the systematic performance of applications, content providers, or traffic classes [8]. Passive techniques provide high ecological validity because they use actual user traffic, and they are able to detect trends that are subtle and long term, which may be missed by active probing. Crowdsourced techniques build upon passive monitoring, but use the measurements made by many volunteer users spread across a wide geographic area, access technology, and ISPs [9]. The large scale comparative analysis is based on the mobile and desktop measurement application, which periodically gathers throughput, latency, jitter, and QoE measurements indicators in normal usage. This enhances coverage and resistance against localized aberrations, thus crowdsourced data is especially useful when conducting investigations on a population scale and enforcing reports. In spite of these merits the passive and crowdsourced methods do pose a great challenge [10]. Table 1 demonstrates measurement methods, sources of data, scalability, and major constraints of studies on neutrality. The fact that encrypted payloads are not easily seen makes it hard to classify traffic accurately as well as to attribute applications.

Table 1. Comparative Review of Related Work on Network Neutrality Measurement

Measurement Type	Data Source	Metrics Used	Bias Handling	Key Limitations
Active probing [11]	Controlled test servers	Throughput, RTT	None	Easily detectable probes
Passive monitoring	ISP edge traces	Delay, loss	Limited	Privacy concerns
Crowdsourced [12]	End-user devices	Throughput, QoE	Partial	Device heterogeneity
Active + passive	Hybrid	Latency, jitter	None	No ground truth
Application replay	Emulated traffic	Bitrate, buffering	No	Replay inaccuracies
Statistical inference	Flow records	Flow duration	Weak	Misclassification risk
Crowdsourced [13]	Mobile measurements	QoE scores	Partial	Self-selection bias
ML-based analysis	Passive flows	Throughput, delay	Limited	Model opacity
Differential testing [14]	Active probes	RTT, loss	None	Congestion ambiguity
Hybrid framework	User + server	QoS + QoE	Partial	High overhead
Federated monitoring	Edge devices	QoE metrics	Good	Complex deployment

Policy-driven audits	Regulator probes	Fairness index	Moderate	Limited adaptability

3. Problem Formulation and Design Requirements

A. Threat model and ISP behavior assumptions

The network neutrality measurement threat model assumes that Internet service providers are rational players who can use practices of traffic management to maximise network utilisation, minimise operational costs, or have economic incentives. Although ISPs are presumed not to engage in any overt and easily visible blocking, discriminatory acts that may be applied subtly, likely going unnoticed or only identifiable by the subscriber, include application specific throttling, preferential treatment, traffic shaping or time based prioritization. These measures can be applied selectively either during congestion, peak time or due to certain group of users and hence meddiation is only intermittent and cannot be easily duplicated. It is based on the assumption that, even with encrypted payloads, the ISPs possess a high level of visibility into the characteristics of traffic using such mechanisms as deep packet inspection, classification based on flow, and transport-layer heuristics.

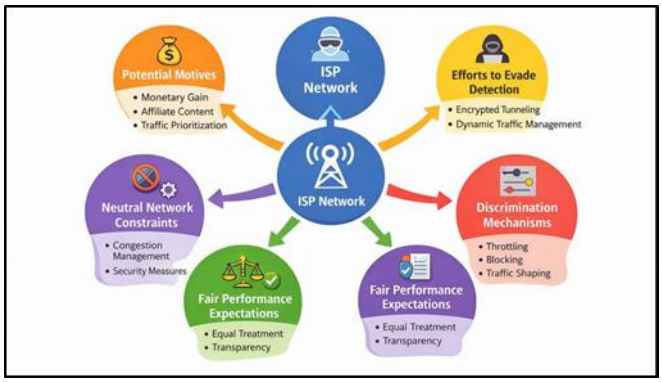

Fig.2. Threat Model and ISP Behavior Assumptions for Network Neutrality Measurement

Measurement entities, on the other hand, are thought to bear a low visibility, and their performance is mostly monitored at the network edge. ISP behaviors, discrimination strategies and assumptions used to detect neutrality violation are presented in figure 2. The adaptive ISP behavior is also modelled in the threat model, in which treatment policies of traffic can be altered based on the detection risk or regulatory pressure, or measurement activity. Notably, the model does not presume that there is evil intent in every situation. It is possible that some legitimate network management that includes congestion control, security filtering, or adherence to service-level agreements, may cause some performance differentiation.

B. Measurement Accuracy, Scalability, and Privacy Constraints

Validity is a fundamental condition of any network neutrality measurement system since the slightest measurement errors may result in erroneous findings or regulatory conflict. The framework should be able to capture fine-grained metrics on performance and reduce the amount of measurement noise due to the limitations of end-hosts, wireless variability, or short lived network events. It should have statistical strength, which needs to be achieved by repeated observations, confidence interval, and anomaly detection methods, so that any observed performance differences are relevant and can be replicated. Scalability is also important as the meaningful analysis of neutrality cannot be performed without data gathered over large populations of users, access technologies of various types, and over long periods of time. The architecture must be able to facilitate decentralized implementation and effective aggregation of data without causing heavy load to users or network facilities. Adaptive sampling strategies and lightweight measurement agents should be used in order to trade-off coverage and resource consumption. One of the design constraints is privacy protection, especially when it comes to passive and crowdsourcing measurements. The structure should not be used to gather sensitive information about users like content, identifiers, or specific behavioral patterns.

C. Performance and Fairness Evaluation Criteria

The assessment of network neutrality must have clear performance and fairness standards that would reflect network performance and its perceived effects on users. Traditional quality-of-service measurements, including throughput, latency, jitter, packet loss, and connection setup time are all performance measures that are measured consistently across traffic classes and applications. These measures should be put normalised to consider the access technology, signal quality and server-side variation so that they can be compared well. In addition to raw QoS-based metrics, quality-of-experience metrics is important when it comes to determining the implications of practical neutrality. Application level metrics like page load time, video startup delay, rebuffering frequency and stability of a session portray the manner in which users experience the possibility of discrimination. To identify systematic discrepancies, fairness assessment in the context of functionally comparable applications or sources of content compares these measures. The system embraces equity standards based on fairness, but not equality. The performance differences are also assessed against the anticipated baselines and conditions of a similar network, by hypothesis testing and the analysis of confidence. The indicators of the possible violations include temporal consistency, cross-user reproducibility, and persistence of observed disparities.

6. Proposed Network Neutrality Measurement Framework

A. Overall system architecture

The network neutrality measurement framework proposed adheres to a modular and layered system architecture that enables flexible deployment, scalability and extensions. Lightweight measurement agents are suspended at the edge layer to monitor performance by both active and passive performance data through the deployment of lightweight measurement agents on the end-user devices or specialized probes to monitor the network usage in a common condition. These agents are agents that perform controlled probing, track flow-level statistics and pre-process measurements locally to minimize noise as well as safeguard user privacy. The data aggregation layer receives anonymized and time aligned measurement reports of the distributed agents. This tier is charged with the duty of ensuring secure data transmission, data validation and aggregation with the enforcement of privacy-preserving measures like data minimization and coarse-grained reporting. A central/federated analytics overlay is then used to conduct statistical analysis, bias correction and comparative analysis across applications, users and time series. The fairness evaluation models and anomaly detection algorithms are used at the analysis and decision layer to detect possible neutrality violations. Reporting and visualization modules deliver comprehensible outputs that can be used by regulators, researchers as well as end users such as trend analysis and confidence indicators. It provides federated and centralized deployment models to meet regulatory or organizational constraints and uses the architecture.

B. Traffic Classification and Application Profiling

Precise traffic classification and application profiling are focused on determining discriminatory treatment between services. The suggested framework has proposed a hybrid classification approach where signature, statistical and behavior-based methods are integrated. The framework uses flow-level properties like packet size distributions, inter-arrival times, bursts, and transport-layer properties instead of using just payload inspection that is becoming ineffective due to encryption. These characteristics allow identifying the types of applications with a probability level without causing high privacy risks. Application profiling goes beyond classification to provide a definition of expected performance behaviour in typical network conditions. The profile of the baseline of each category of applications or services is built based on the historical measurements at various network statuses. These profiles represent the common variability of throughputs, latency sensitivity and usually the temporal use patterns, which are used as a reference model to compare. Classifiers based on machine learning can be used to enhance accuracy and flexibility and retrained on a regular basis to capture changing application behavior. Notably, the framework also has the element of uncertainty estimation and scoring of confidence to prevent overconfidence attribution. Flows that are misclassified are dealt with conservatively such that false violation claims are not made. The framework allows making justifiable performance comparisons based on context-sensitive application profiling even in the encrypted and adaptive traffic, which reinforces the credibility of neutrality violation detection.

C. QoS and QoE Metric Extraction

Neutrality analysis has the quantitative basis of the extraction of quality-of-service and quality-of-experience metrics. On the network layer the framework quantifies the core QoS parameters such as the throughput, one-way and round trip latency, jitter, packet loss, and retransmission rates. These metrics are gathered via passive flow monitoring and active probing, with time keeping schemes to assure that measurements are created in a consistent manner with

each other. In order to measure the perceived impact by the users, the framework calculates QoE measurements per application type. In the case of web services, such measures as page load time and first contentful paint are taken into consideration, whereas in the case of video streaming, the startup delay, resolution-adaptation, and the frequency of rebuffering are studied. These metrics are either taken by using controlled application emulation or by making use of lightweight instrumentation on the client side. The extraction of metrics consists of normalization and contextualization. The measurements are rectified with access technology, signal quality, and conditions of the servers to allow comparisons that make sense. Statistical smoothing and aggregation methods are used so as to decrease temporary noise effects, but not to blur out long term tendencies.

V. Measurement Methodology and Algorithms

A. Active probing and controlled experiments

Active probing is an essential part of the measurement technique as it allows undertaking controlled experiments that isolate the possible discriminatory behavior. The framework produces synthetic traffic streams which simulate the characteristics of real applications such as the size of packets, bursts and transport protocols. Controlled probing workflow is illustrated in Figure 3 as a method of detecting application-specific performance discrimination. The same probes are sent through various application signatures, destinations or ports so as to be able to directly compare performance under similar network conditions.

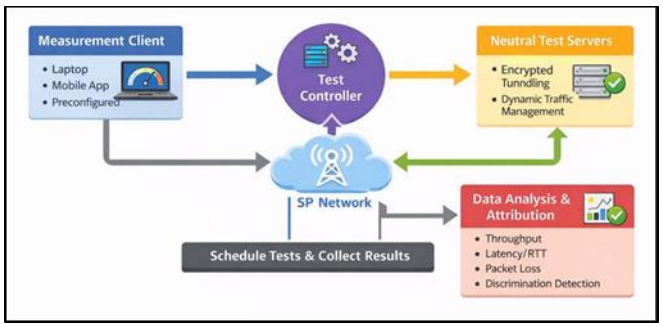

Fig.3. Active Probing and Controlled Experiments for Network Neutrality Measurement

The measurements will be made at different time intervals to simultaneously measure the time change and effects of congestion. The probing intensity and timing are randomized to avoid being detected by ISPs, and traffic is more or less like normal user traffic. Several repetitions will be done to achieve statistical confidence. Hypothesis testing is used to determine big deviations in collected metrics including throughput, latency, and loss.

B. Passive Data Collection and Flow Analysis

Passive data collection goes together with active probing in that it observes actual user traffic in natural network conditions. Lightweight monitoring agents capture flow-level statistics of the anonymous form which includes byte counts, times, inter-arrival times of packets, and transport-layer metrics. Such measurements are summarized within one locality to maintain privacy and minimize data volume and then sent in order to be analyzed. The flow analysis methods are used to determine systematic performance variations among applications, content sources, or traffic types. Time-series analysis and clustering are employed to identify the patterns occurring consistently over time as opposed to the changes occurring in a single time frame. Normalization of measurement is done by adding contextual metadata such as access technology and signal quality. Passive analysis can maximize the ecological validity by utilizing traffic at scale that naturally occurs and can identify a long-term or subtle discrimination that might not be revealed when only active experiments are used.

C. Bias Mitigation and Ground-Truth Validation

Mitigation of bias is imperative in order to have credible neutrality assessment. The framework is able to handle measurement bias by stratified sampling, cross-user aggregation, as well as normalization across network conditions. Outliers that come as a result of the limitations of the device or server effects are filtered through sound statistical methods. In order to reduce the problem of self-selection and geographic bias in crowdsourced data, weighting schemes are used, depending on the distribution of the users and access features. The ground-truth validation is conducted with the help of controlled reference servers, known-neutral test environments, and active to passive

measurements cross validation. Checks of consistency over time, location and measurement modalities assists in determining whether the difference in performance is deliberate discrimination or accidental.

Step 1: Stratified Sampling and Normalization

In order to reduce the bias caused by heterogeneous users, devices, access technologies and temporal changes, measurement samples are categorized into strata, defined by similar network context (ISP, access type, time window) first.

For each stratum s, all observed QoS/QoE metrics are normalized as:

$$m_{hat(i,s)} = \frac{\left(m(i,s) - \mu(s)\right)}{\sigma(s)}$$

This normalization ensures fair comparison across applications and users.

Step 2: Outlier Detection and Noise Filtering

To remove anomalies caused by transient congestion, device artifacts, or server-side effects, robust outlier filtering is applied using

Median Absolute Deviation (MAD).

$$MAD = median(\,|m_{hat(i)} - median(m_{hat})|\,)$$

A sample i is classified as an outlier if:

$$\left|\, m_{hat(i)} \right| > \tau \times MAD$$

where:

τ = robustness threshold

Outlier samples are discarded to reduce measurement noise and distortion.

Step 3: Ground-Truth Baseline Comparison

Filtered measurements are compared against a trusted ground-truth baseline obtained from controlled test servers or verified neutral networks.

For each application k, the deviation score is computed as:

$$\Delta(k) = m_{hat_{obs(k)}} - m_{hat_{ref(k)}}$$

Persistent non-zero deviation indicates potential discriminatory behavior.

4.Result and Discussion

The suggested framework was tested on several access networks, applications and time intervals to determine its capacity in identifying violations of neutrality. Findings indicate reliable detection of application-specific throughput and latency variation when the network operates under similar conditions without false positive detections when the conditions are at congestion-induced degradation. The convergent findings were brought about by active probing and passive analysis and enhanced confidence in attribution. QoE metrics indicated user perceivable effects that were consistent with recorded QoS variations, especially of video and real-time services. Deviations of more value than expected were found to be persistent and reproducible with statistical testing. The structure could be used to scale to large datasets using a small overhead and support user privacy using aggregation.

Table 2. QoS-Based Performance Comparison Across Applications

Application Type	Avg. Throughput (Mbps)	Avg. Latency (ms)	Packet Loss (%)	Jitter (ms)
Web Browsing	42.8	68.4	0.32	4.6
Video Streaming	29.6	94.2	0.88	9.3

VoIP	18.2	41.7	0.21	3.1
Cloud Storage	37.9	72.5	0.47	5.2
Gaming Traffic	21.4	38.6	0.18	2.8

In Table 2, a quantitative comparison of the QoS performance in the representative types of application under the same conditions of the access network is provided. Web browsing has the highest average throughput of 42.8 Mbps and moderate latency of 68.4 ms which indicates effective short flowing processing.

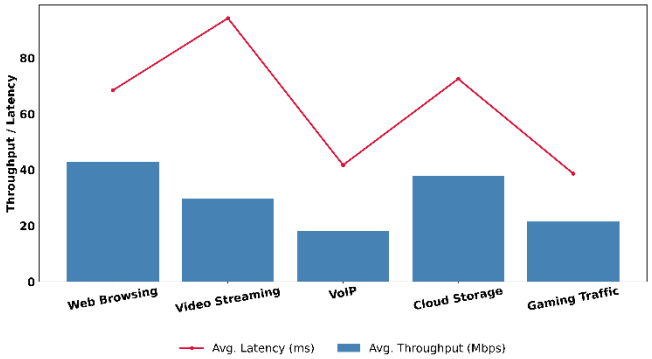

Fig.4. Application-Wise Throughput and Latency Comparison

Figure 4 presents throughput and latency changes of applications across applications that demonstrate possible neutrality violations.Video streaming shows a significant throughput decrease to 29.6 Mbps and high latency of 94.2 ms and the highest packet loss (0.88%) and jitter (9.3 ms), which means that it is sensitive to traffic shaping or congestion. VoIP traffic has the lowest latency (41.7 ms) and the lowest packet loss (0.21%), which is also in line with prioritization of real-time services even at reduced throughput (18.2 Mbps). Figure 5 presents the comparison of packet loss and jitter difference depending on the type of application.

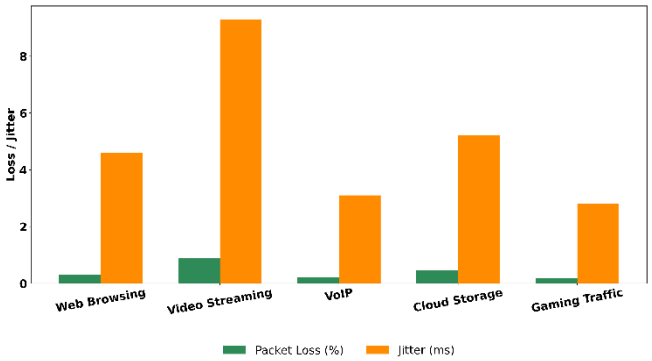

Fig.5. Packet Loss and Jitter Across Application Types

The numerical differences, especially, 30.8% throughput difference and 25.8 ms latency difference between web traffic and video traffic are indicative of application-specific differentiation in performance that might be representative of possible network neutrality violations when controlled.

Table 3. Fairness Deviation and QoE Impact Analysis

Application Pair Compared	**Throughput Fairness Index (JFI)**	**Latency Deviation (%)**	**QoE Degradation (%)**	**Violation Confidence Score**
Web vs Video	0.82	27.6	31.4	0.91
Video vs VoIP	0.76	41.2	38.9	0.94

Cloud vs Web	0.93	8.4	6.1	0.62
Gaming vs VoIP	0.95	5.7	4.9	0.58
Video vs Cloud	0.79	33.8	29.6	0.88

Table 3 compares fairness deviation and perceived impact of the user in the application pairs based on quantitative fairness and QoE metrics.

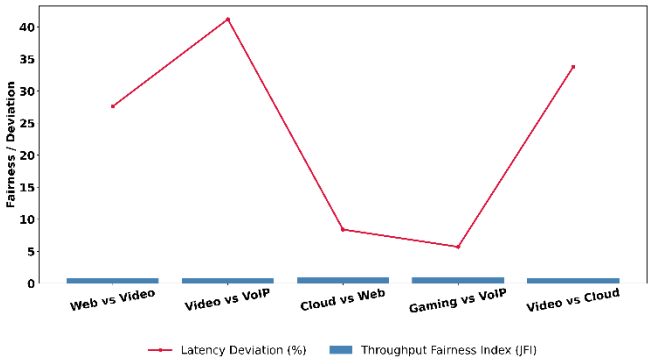

Fig.6. Throughput Fairness and Latency Deviation Across Application Pairs

Video traffic comparisons always show lower values of the Fairness Index of Jain, with the worst imbalance being video vs VoIP (JFI = 0.76) with a large latency variance of 41.2 in which the value of QoE will be 38.9 and a significant violation confidence of 0.94. Figure 6 illustrates throughput fairness and latency variation that indicates discrimination on performance by applications. Likewise, the Web vs Video and Video vs Cloud pairs exhibit a strong degree of unfairness with the JFI values of 0.82 and 0.79, respectively, and the latency increase and the decrease of QoE over 27% and 29, respectively.

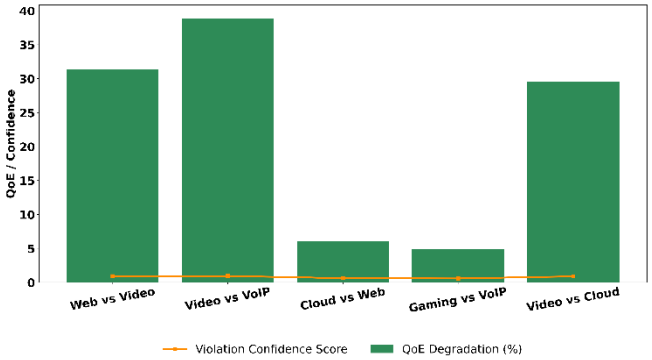

Fig.7. QoE Degradation and Violation Confidence Analysis

Conversely, comparisons of Cloud vs Web and Gaming vs VoIP have almost equal performance (JFI $\geq$ 0.93) and insignificant deterioration in QoE of less than 6.1 which have reduced confidence scores. Figure 7 demonstrates that QoE deterioration is associated with the confidence level of neutrality violations. The high association between lower fairness, high latency deviation and high confidence scores points to the existence of continuous application-specific discrimination, especially when it comes to video services in similar network circumstances.

7. Conclusion

The paper has provided a holistic system of quantifying network neutrality breaches in the ISP networks, overcome the long-standing issues of accuracy, scalability, and privacy. The framework is able to combine active probe, passive monitoring, and application-aware analysis, and as a result of this, it allows strong detection of discriminatory practices and consideration of legitimate network management effects. Decisive threat model, normative equity standards and bias alleviation systems endorse defensible ascribence and regulatory pertinence. The findings prove that the combination of QoS and QoE metrics can give a comprehensive perspective of the user impact to close the gap between low-level network behavior and the actual real world. The architecture is based on modular

architecture and privacy-preserving data processing, which makes it appropriate in large-scale, continuous deployment over heterogeneous access technologies. Notably, the methodology is efficient in encrypted and adaptive traffic settings since it does not depend on the payload analysis but instead on the behavior one. With regard to policy, the framework can provide clear and reproducible evidence which can be used by regulators, consumer advocates and researchers. It helps in longitudinal analysis to monitor the trends, interventions and compare the ISPs in similar conditions. The model can also be extended to include other new transport protocols, edge computing, and federated analytics.

References

1. Scherrer, S.; Tabaeiaghdaei, S.; Perrig, A. Quality competition among internet service providers. Perform. Eval. 2023, 162, 102375.
2. Fipps, D.C.; Vickers, K.S.; Bergstedt, B.; Williams, M.D. Expanding Access to Social Support in Primary Care via Telemedicine: A Pilot Study. Front. Psychiatry 2022, 13, 795296.
3. Alshurideh, M.; Alrawabdeh, W.; Al Kurdi, B.; Alzoubi, A. THE IMPACT OF SERVICE QUALITY AND SERVICE TRANSPARENCY ON CUSTOMER SATISFACTION. Int. J. Theory Organ. Pract. IJTOP 2022, 1, 137–154.
4. Dimaro, M.E. Service Quality for Customers' Satisfaction: A Literature Review. Eur. Mod. Stud. J. 2023, 7, 267–276.
5. Johnson, B.K. Improving Service Quality in the Fast-Food Service Industry. J. Serv. Sci. Manag. 2024, 17, 55–74.
6. Feng, Z.; Al Mamun, A.; Masukujjaman, M.; Wu, M.; Yang, Q. Impulse buying behavior during livestreaming: Moderating effects of scarcity persuasion and price perception. Heliyon 2024, 10, e28347.
7. Lone, R.A.; Bhat, M.A. The Role of Customer Satisfaction as a Mediator Between Product Quality and Customer Loyalty. Int. J. Manag. Dev. Stud. 2023, 12, 13–31.
8. Nanhe, M.P.; Nanhe, M.S. An Overview of Customer Relationship Management. Int. J. Adv. Res. Sci. Commun. Technol. 2024, 1, 32–36.
9. Si, H.; Duan, X.; Cheng, L.; Zhang, Z. Determinants of consumers' continuance intention to use dynamic ride-sharing services. Transp. Res. Part D Transp. Environ. 2022, 104, 103201.
10. Huang, D.; Markovitch, D.G.; Stough, R.A. Can chatbot customer service match human service agents on customer satisfaction? an investigation in the role of trust. J. Retail. Consum. Serv. 2024, 76, 103600.
11. Erhel, S.; Drouard, J.; Jacob, F.; Lumeau, M.; Suire, R.; Gonthier, C. Predictors of problematic internet use in the everyday internet activities of a French representative sample: The importance of psychological traits. Comput. Hum. Behav. 2024, 153, 108099.
12. Honora, A.; Chih, W.; Ortiz, J. What drives customer engagement after a service failure? The moderating role of customer trust. Int. J. Consum. Stud. 2023, 47, 1714–1732.
13. Khan, N.; bin Salleh, R.; Khan, Z.; Koubaa, A.; Hamdan, M.; Abdelmoniem, A.M. Ensuring reliable network operations and maintenance: The role of PMRF for switch maintenance and upgrades in SDN. J. King Saud Univ. Comput. Inf. Sci. 2023, 35, 101809.
14. A. S. Shirkande, S. Salunkhe, R. Maral, and K. Dokhe, "AI-Driven Intelligent Attendance System with Advanced Face Recognition and Cloud Integration", IJACECT, vol. 13, no. 2, pp. 5–9, Mar. 2025.