# Machine Learning For Network Traffic and Video Quality Analysis

Develop and Deploy Applications Using JavaScript and Node.js

—

Tulsi Pawan Fowdur
Lavesh Babooram

Apress®

# Machine Learning For Network Traffic and Video Quality Analysis

## Develop and Deploy Applications Using JavaScript and Node.js

**Tulsi Pawan Fowdur**
**Lavesh Babooram**

Apress®

## *Machine Learning For Network Traffic and Video Quality Analysis: Develop and Deploy Applications Using JavaScript and Node.js*

Tulsi Pawan Fowdur
Department of Electrical and Electronic Engineering, University of Mauritius, Reduit, Mauritius

Lavesh Babooram
Reduit, Mauritius

ISBN-13 (pbk): 979-8-8688-0353-6
ISBN-13 (electronic): 979-8-8688-0354-3
https://doi.org/10.1007/979-8-8688-0354-3



Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Celestin Suresh John
Development Editor: Laura Berendson
Coordinating Editor: Gryffin Winkler
Copy Editor: April Rondeau

Cover designed by eStudioCalamar

Cover image by Joshua Fuller on Unsplash (www.unsplash.com)

Distributed to the book trade worldwide by Apress Media, LLC, 1 New York Plaza, New York, NY 10004, U.S.A. Phone 1-800-SPRINGER, fax (201) 348-4505, email orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC, is a California LLC, and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub (https://github.com/Apress). For more detailed information, please visit https://www.apress.com/gp/services/source-code.

If disposing of this product, please recycle the paper

# Table of Contents

# About the Authors

**Dr. Tulsi Pawan Fowdur** received his bachelor of engineering degree in electronic and communication engineering with honors from the University of Mauritius in 2004. He was also the recipient of a gold medal for having produced the best degree project at the Faculty of Engineering in 2004. In 2005, he obtained a full-time PhD scholarship from the Tertiary Education Commission of Mauritius and was awarded his PhD in electrical and electronic engineering in 2010 by the University of Mauritius. He is also a registered chartered engineer of the Engineering Council of the United Kingdom, fellow of the Institute of Telecommunications Professionals of the United Kingdom, and a senior member of the IEEE. He joined the University of Mauritius as an academic in June 2009 and is presently an Associate Professor at the Department of Electrical and Electronic Engineering of the University of Mauritius. His research interests include mobile and wireless communications, multimedia communications, networking and security, telecommunications applications development, the Internet of Things, and artificial intelligence (AI). He has published several papers in these areas and is actively involved in research supervision, reviewing papers, and also organizing international conferences.

**Lavesh Babooram** received his bachelor of engineering degree in telecommunications engineering with networking with honors from the University of Mauritius in 2021. He was also awarded a gold medal for having produced the best degree project at the Faculty of Engineering in 2021. Since 2022, he has been pursuing a master of science degree in applied research at the University of Mauritius. With in-depth knowledge of telecommunications applications design, analytics, and network infrastructure, he aims to pursue research in networking, multimedia communications, Internet of Things, artificial intelligence, and mobile and wireless communications. He joined Mauritius Telecom in 2022 and is currently working in the Customer Experience and Service Department as a pre-registration trainee engineer.

# About the Technical Reviewer

**Kamalakshi Dayal** received a bachelor of engineering degree in telecommunications engineering with networking, with first-class honors, from the University of Mauritius in 2021. She then undertook a one-year internship at Huawei Technologies (Mauritius) Ltd., whereby she had the opportunity to work on two highly innovative and ground-breaking award-winning projects, assessed at the regional level. She is currently an engineer at the company and is specializing in a multitude of product lines, mainly in convergent billing systems, IPTV, and cloud services.

CHAPTER 1

# Introduction

This chapter introduces the concepts of network traffic monitoring and analysis (NTMA) and video quality assessment (VQA). It discusses the significance of NTMA and VQA in modern telecommunications by emphasizing the need to achieve optimal network performance and to boost user experience, which encompasses both the flow of network parameters and the video streaming quality. The sections in this chapter set the tone for the implementation phase by first exploring the need for NTMA and VQA with regard to preserving the quality of service (QoS) in different network environments. With the aim of executing these processes on any device irrespective of the operating system, a combination of machine learning (ML), JavaScript, and Java, with Node.js and Apache HTTP Server as the backend frameworks, is used. Network traffic parameters are read from the local device before streamlining client–server interactions to produce meaningful prediction and classification results. Likewise, a combination of distortion artifacts is applied to a playing video to produce a video quality score. The following sections provide an overview of the book's structure and offer a glimpse into what will be covered in the next chapters.

## 1.1 Overview of Network Traffic Monitoring and Analysis

NTMA is a cornerstone of today's telecommunications environment, essential for ensuring network efficiency, security, and user experience. The exponential rise of digital interactions, exacerbated by the introduction of 5G and the Internet of Things (IoT), emphasizes the need to monitor and regulate network traffic patterns. NTMA serves as a watchdog in the networking biosphere, actively monitoring the changing patterns of data streams. This heightened surveillance is motivated by the primary goals of assessing traffic conditions, identifying anomalies, and improving performance to provide consumers with a smooth digital experience [1].




T. P. Fowdur, L. Babooram, *Machine Learning For Network Traffic and Video Quality Analysis*,
https://doi.org/10.1007/979-8-8688-0354-3_1

Statistics from industry publications shine a bright light on the scope of NTMA. According to Cisco's Annual Internet Report, worldwide IP traffic was expected to triple to 396 exabytes per month by 2022, a threefold increase from 2017 [2]. In an era when a massive amount of multimedia content is consumed at lightning speed, NTMA proves to be a fundamental aide for telecommunications operators as they not only decode intricate traffic trends but also anticipate and mitigate network congestion, bottlenecks, and possible security breaches.

Within the NTMA paradigm lies a whole range of complexities, starting with the diverse nature of internet traffic. This jumbled and disorganized mix contains packet headers, payload data, and metadata, all originating from different multimedia streams. Putting this mosaic of information under the analytics microscope offers insights into the transmission dynamics among devices, applications, and services, shedding light on patterns that might otherwise go unnoticed and unreported. However, it is computationally and mathematically intensive to yield meaningful information from the colossal amount of traffic that traverses a typical network, often exceeding billions of packets per second. Adding to the list of hurdles is the encrypted nature of communication packets, which hides critical information, thus further necessitating complex approaches for useful analysis.

The real-world ramifications of NTMA are numerous and multifaceted. For example, NTMA serves as a pillar in network operations centers (NOCs) and service operations centers (SOCs), where it assists in the rapid identification of harmful activity, the prevention of data leaks, and the protection of sensitive assets [3]. Likewise, NTMA improves quality of service (QoS) concerning network optimization by dynamically and proactively monitoring and reporting network congestion sites and rerouting traffic. Another poll by Spiceworks indicated that 53 percent of information technology (IT) professionals perceive NTMA to be the most pivotal component of maintaining their infrastructure, highlighting the need for service providers to evaluate user experiences in real time and guarantee seamless connectivity [4].

As NTMA transitions through this period of heightened technological change, machine learning (ML) has emerged as a powerful ally. ML propels NTMA to previously unattained heights, using cutting-edge algorithms to fuel predictive abilities, robust anomaly detection, and responsive network management. On the same wavelength, the adaptability of ML frameworks with regard to being lightweight, compact, fast, and efficient acts as the pillar upholding the capability of the typical end user to perform

NTMA at the client's side. This revolutionizes digital ecosystems, allowing the end user to be equipped with high-performing algorithms to gauge the reception quality of multimedia content, resulting in a more sophisticated and complete ecosystem.

NTMA can be represented as a layer between network components and SOC and NOC platforms, as illustrated in Figure 1-1.

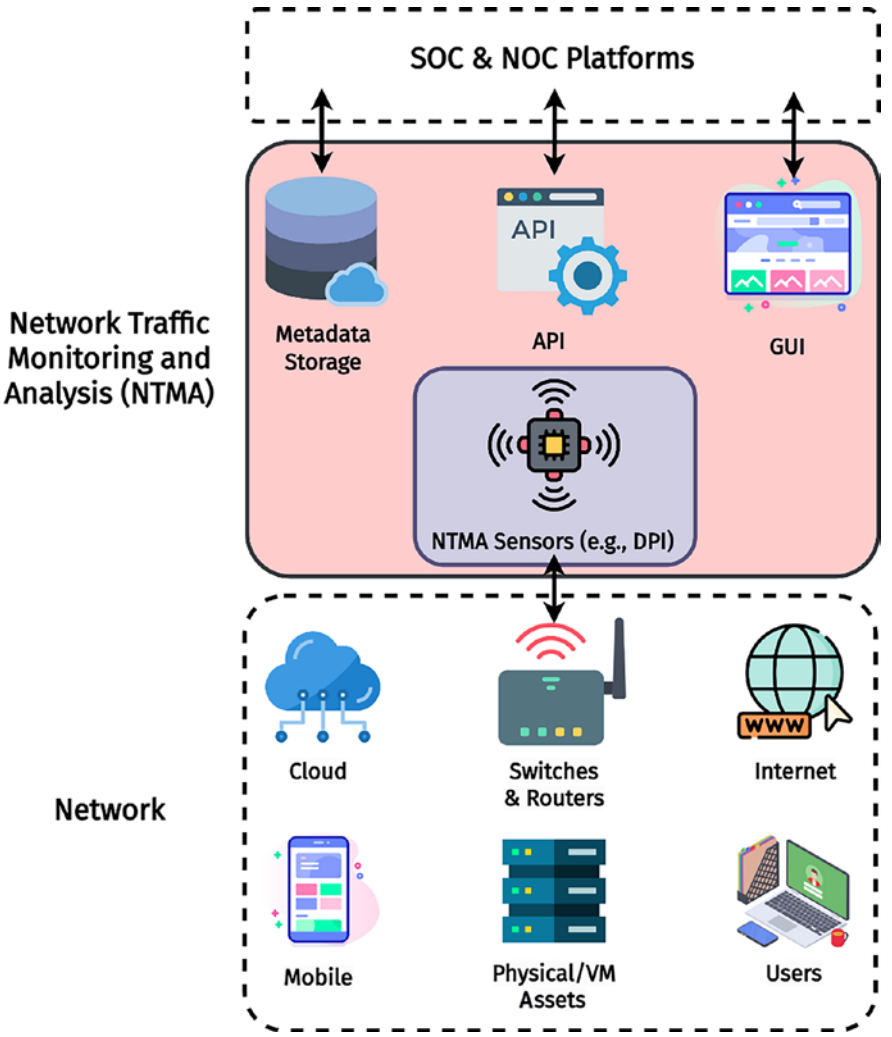


***Figure 1-1.*** *NTMA layer in modern frameworks*

The following sections elaborate upon the different aspects that make up NTMA, such as its necessity and perks.

### 1.1.1 Importance of NTMA

NTMA stands out like a sentinel in the complex web of today's telecommunications, keeping tabs on the virtual veins that supply the interconnected world. As digital interactions become ubiquitous, the sheer quantity of data moving across networks has skyrocketed. International Data Corporation (IDC) estimates that worldwide internet users will create 175 zettabytes by 2025 [5]. NTMA is the guardian of network security, privacy, and efficiency in the face of an ever-increasing data flood.

One of the primary goals of NTMA is to make sense of the random nature of network traffic, which from a global perspective is a chaotic jumble of different kinds of interactions, data flows, and endpoints. Firstly, by describing these patterns, NTMA offers network managers a solid base from which to begin improving performance, and secondly, by spotting anomalies and deviations from the preset norms, NTMA ensures alarms and notifications can be triggered during possible security breaches and interruptions [6].

A distributed denial of service (DDoS) assault may be imminent if data packets suddenly increase in volume from a specific geographical location. The strength of NTMA is not only in its capacity to spot this aberration but also in its readiness to act swiftly to limit the damage it causes. The threat environment is changing, with the number of recorded DDoS assaults having increased by 67 percent in 2022 compared to the previous year, as reported by Cloudflare. Kaspersky also registered nearly 58,000 such incidents [7]. As such, NTMA serves as a digital lighthouse, allowing network experts to remain vigilant against new threats and quickly restore normality after a compromise. The sheer volume of data being sent also calls for strategic use of resources and careful network optimization. With NTMA's help, ISPs and other telcos may pinpoint impediments, ease traffic, and distribute bandwidth more effectively. This is significant because the demand for telecommuting jobs, online courses, and digital media has been on the rise ever since the pandemic in 2020. As a result of NTMA's work to improve QoS, customers can enjoy a more consistent digital experience, with HD video streaming, page loads, and app responsiveness all functioning at peak efficiency.

To sum up, NTMA is more than just a monitoring process; it also improves network security and makes users satisfied. Its pervasiveness is highlighted by the prevalence of digital interactions, and its significance will grow as networks mature. NTMA paves the way for a digitally linked society that lives on efficiency and dependability by welcoming the diversity of network traffic, comprehending its subtleties, and converting them into useful information.

## 1.1.2 Key Objectives of NTMA

At its core, NTMA aims to tick several boxes of network management and optimization. As the number of digital contacts continues to grow, with a recorded 5.44 billion internet users as of April 2024, according to Statista [8], NTMA will play an increasingly important role in ensuring the continued viability, safety, and efficiency of today's networks. Strategically, NTMA aims to do the following [9]:

- Describe typical traffic flows and data streams at the application level.
- Identify outliers and anomalies proactively.
- Enhance overall efficiency through optimal routing.
- Observe traffic trends and forecast traffic for different network environments.
- Provide a bird's-eye view of the network.

Telecommunications experts may get invaluable insights into the patterns that characterize network activity thanks to NTMA's rigorous categorization and analysis of the various data streams crossing networks. Anomaly detection, the pre-emptive detection of abnormalities from established traffic standards, relies on this familiarity with normality as its foundation. For instance, VMware Carbon Black reported a 118 percent rise in assaults against banking firms in 2020 [10]. The ability of NTMA to detect abnormalities, including unexpected increases in traffic or changes in communication patterns, is crucial to preventing security breaches. As the quantity and significance of digital interactions grow, NTMA is a natural fit with the need to optimize networks. To improve QoS and resource management, NTMA identifies areas of overcrowding, traffic limitations, and other performance constraints. This is especially important now since the average internet speed throughout the world is expected to reach 110.4 Mbps by 2023, as reported by Ookla [11]. Users now demand consistent, low-latency, high-speed access, which is upheld by NTMA's features. NTMA is thus the nexus at which security, efficiency, and user experience all meet, and addresses the complexities of network dynamics. The goals can be summarized as protecting the delicate balance between the ever-increasing amount of data and the need for a seamless user experience, which reverberates more strongly as digital ecosystems evolve.

## 1.1.3 Network Traffic Components

The backbone of today's communication infrastructure, network traffic is itself a complex phenomenon. Internet Protocol (IP) packet headers offer a background for data transfer by encoding information such as the source and destination addresses and port numbers. Metadata, which provides background information, supplements payload data, which represents the message itself. The wide variety of streaming services, signaling packets, and control messages adds to the already chaotic state of network traffic [12]. The IDC predicts that by 2025 the global datasphere will grow to 175 zettabytes, 75 percent of which will relate to non-PC devices, in turn reflecting the growth of non-PC traffic sources [13]. By dissecting these complex parts, network administrators may learn more about user behaviors, application relationships, and traffic flows. Underneath the surface of frictionless digital exchanges is a tangled web of network traffic. This complex network consists of a symphony of parts, all of which play a role in the seamless transfer of information between computers. Statista predicts that there will be 29.4 billion IoT devices in use throughout the globe by 2030, which means that there will be an exponentially increasing variety and number of network traffic components [14].

Data packets are the building blocks of network traffic. These digital packages transmit data to their final destinations. Like letters in the mail, these packets have unique "headers" that include crucial information, such as where they came from and where they're going, as well as the ports and protocol that they are using. Routers and switches may use this contextual information to send data to the correct destinations. The "payload," or body of a message, is contained even deeper inside these packets. The information itself, such as text, photos, video streams, or application-specific data, is located here during transmission. The foundation of today's digital experiences rests on the fast-paced communication of these packets. Figure 1-2 shows the structure of an IP packet [15].

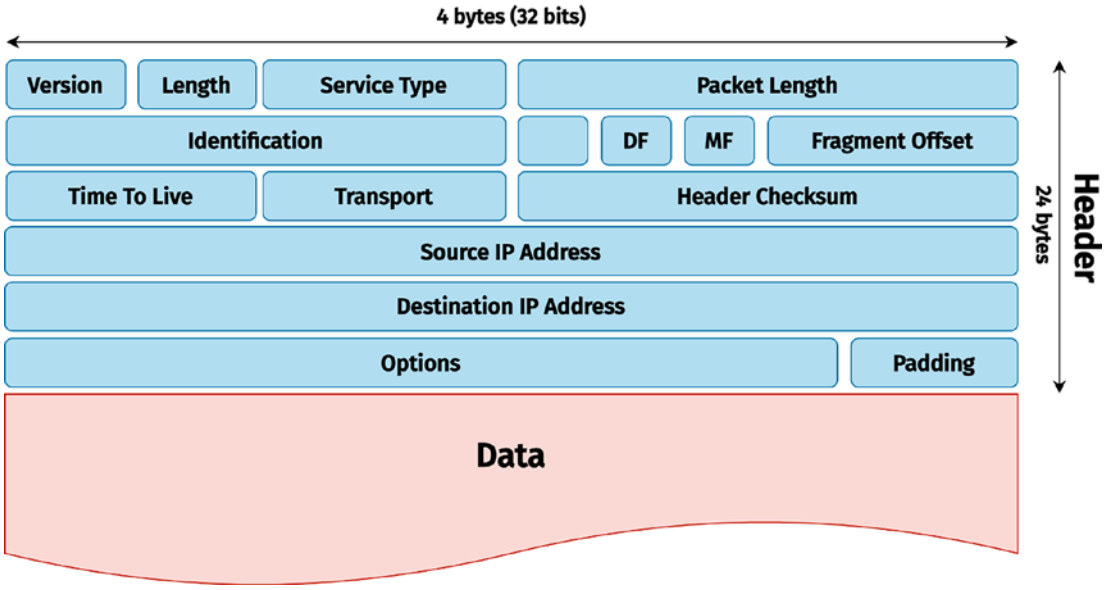


***Figure 1-2.*** *Structure of an IP packet*

Likewise, "flows" of connected packets that share characteristics are highlighted in the network [16]. Network managers can thus comprehend communication dynamics between apps, services, and devices—i.e., at different levels—leading to a bird's-eye view of the network dynamics. This is where the multiverse of stream types also comes into play, where Voice over Internet Protocol (VoIP) conversations, video streaming, and online surfing activities can be segmented and analyzed according to their unique trends. In addition, metadata of packet timestamps, communication length, and transmission sequence numbers further, among others, help to enhance and grasp network interactions.

However, the wide spectrum of network traffic elements poses certain difficulties. The expansion of video media in internet traffic, which Cisco predicted, would account for 82 percent of all IP traffic by 2021 [17] and presents complexities that necessitate advanced traffic analysis methodologies. The complex dance of packet headers, payload data, metadata, and multimedia feeds produces an evolving complex terrain that NTMA attempts to maneuver. Understanding these components is essential for gaining comprehension of user habits, recognizing causes of network congestion, and guaranteeing an unparalleled user experience in a progressively data-driven environment. As of January 2023, Sandvine reported a 24 percent increase in video traffic, with Netflix overtaking YouTube in terms of video consumption. A broad list of traffic categories, together with the total volume by traffic category consumed worldwide by the end of January 2023, is depicted in Figure 1-3 [18, 19].

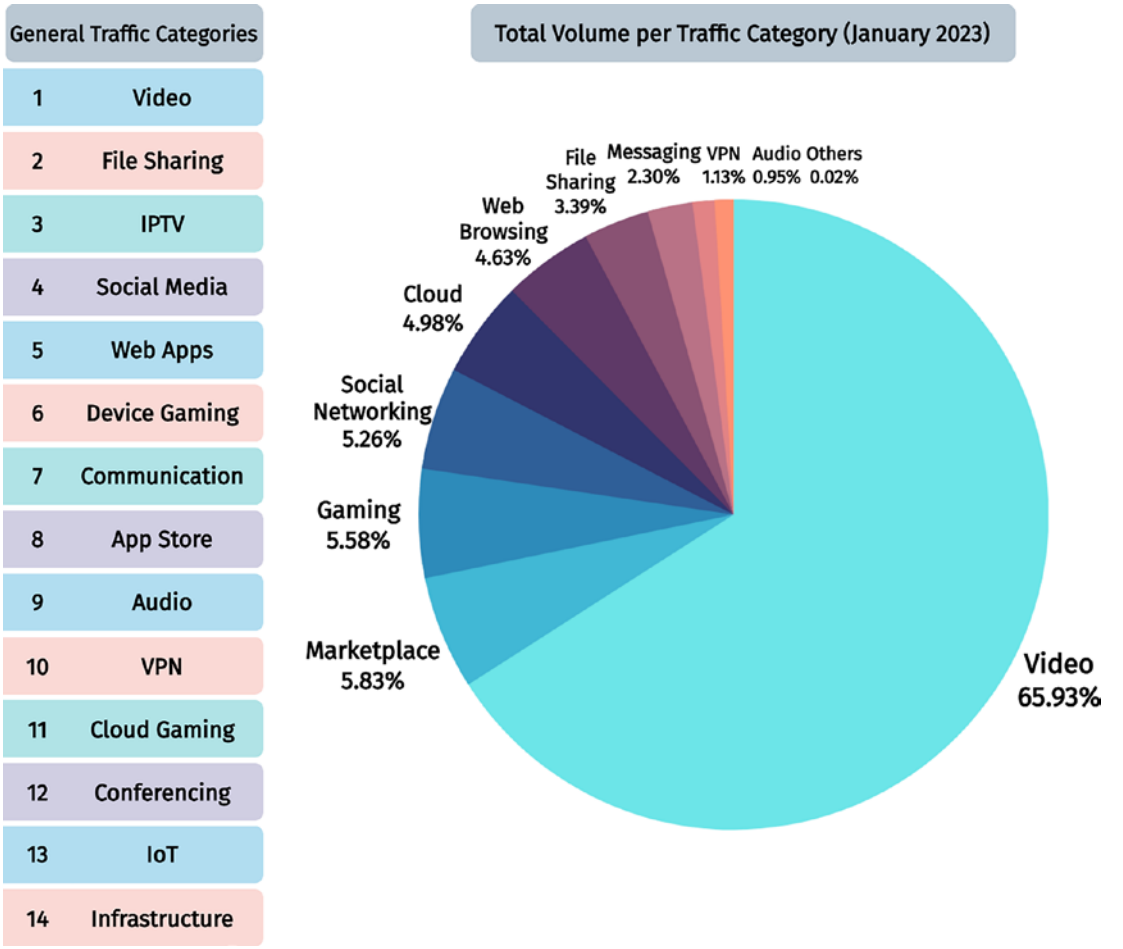


***Figure 1-3.*** *General network traffic categories and total worldwide volume consumption per category*

## 1.1.4 NTMA Techniques and Methodologies

NTMA serves as proof that technological innovation and analytical prowess may successfully coexist. From simple packet capture to powerful ML algorithms, NTMA marches through the raw data maze by allowing telecom engineers and data analysts to mine for useful patterns, irregularities, and conclusions. The concept of capturing packets is at the pinnacle of NTMA techniques. This fundamental approach intercepts and captures data packets as they travel through a network. Network experts obtain open-to-use access to the information contained in packets by capturing them in their

natural form, from headers through payloads [20]. Packet capture is the foundation for understanding communication patterns, analyzing data flow features, and, most important, recognizing abnormalities that may indicate safety issues or connection inconsistencies. This method is analogous to a digitized Rosetta Stone, deciphering the meaning of network connections.

One of the core methods of network analysis revolves around the handling of large floods of network data through a flow-based evaluation, where flows are formed by grouping packets according to shared features, such as source and destination addresses, port numbers, and protocol types [21]. This decoupling allows network managers to make better choices based on accumulated information rather than on individual packets, resulting in a more holistic knowledge of network behavior [22]. The insights are then developed and derived from the behavior of patterns observed at the device, application, and service levels.

As NTMA professionals explore this terrain, two different methods emerge: active network monitoring and passive network monitoring. To measure throughput, safety, and dependability, active network monitoring generates traffic on purpose. Active monitoring is a method of evaluating the state of a network by simulating different situations via the use of "probes" or "agents" to collect data on response times, latency, and other metrics [23]. Similar to a lab experiment, this method allows for unobstructed views into the structure and operation of a network. When availability and responsiveness are mission-critical, active monitoring shines because it allows for a continuous evaluation of the network's behavior and performance. MarketsandMarkets predicts that the worldwide network monitoring market will surpass $6.97 billion by 2030 [24], and the financial industry, for one, uses active monitoring to guarantee that trading platforms react quickly to fluid market developments.

Passive network monitoring, on the contrary, takes the role of a quiet observer, documenting all network activity without adding to the existing volume of data being sent [25]. Techniques like deep packet inspection (DPI) exemplify this approach by letting network managers record and examine traffic in its unaltered condition. When deep historical context into a network's behavior is needed, passive monitoring is preferred. To better allocate resources and optimize their networks, internet service providers (ISPs) often use passive monitoring techniques, such as analyzing patterns in traffic [26].

Moreover, the extra layer of reliability, and high accuracy, is fueled by the adoption of data analysis and ML, which elevate NTMA frameworks to a whole new dimension. The array of ML algorithms provides a comprehensive toolset for recognizing patterns and anomaly detection [27]. Network experts can detect abnormalities that would otherwise go undetected if inference and descriptive statistics were not used [28]. Additionally, predictive analytics and anomaly detection have entered a new age due to the partnership of NTMA and ML. From supervised algorithms to deep learning (DL) architectures, ML models consume enormous datasets to unearth previously hidden correlations and outliers. Having ascended to reach a staggering $6 trillion loss in global cybercrime in 2021, cyberattacks are expected to rise further [29]. This integration with ML can improve threat detection accuracy. Since ML models can change and adapt from erratic network behaviors, NTMA is better able to foresee potential problems, spot outliers, and suggest preventive measures. ML transforms NTMA from a reactive approach to a proactive one, meeting the needs of a modern, data-driven society.

As NTMA advances into an age defined by an overload of information and advanced technology, its methods reflect this rapid transformation. The complex dynamics of network traffic are revealed through the orchestration of insights gained through packet capture, flow-based analysis, statistics, and ML. In an era characterized by connection and knowledge, this symphony arms telecommunications experts with the means to not only understand but also predict network behavior, guiding networking infrastructures toward efficiency, security, and performance. Figure 1-4 depicts the conceptual framework that serves as the foundation for the majority of recent studies on NTMA proceedings [30].

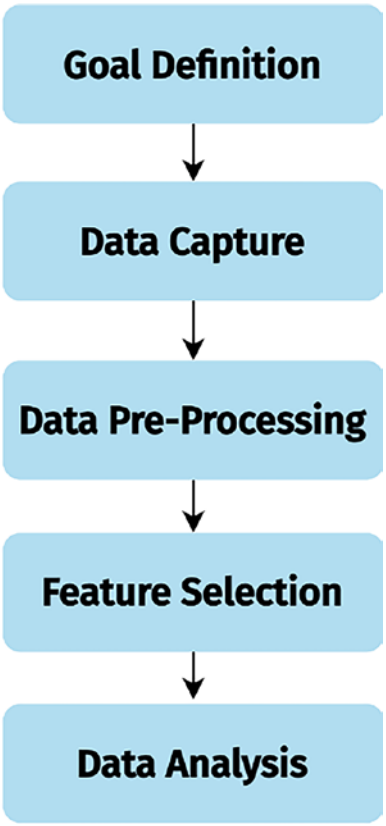


***Figure 1-4.*** *General framework for NTMA procedure*

## 1.1.5 Challenges of NTMA

NTMA is a sentinel amidst the ocean of data flowing through the complex web of today's networks, entrusted with extracting the hidden storylines lying within the massive influx. However, this area of knowledge conceals a maze of obstacles that can only be overcome with creativity, flexibility, and cutting-edge approaches.

One of the primary difficulties is the overwhelming quantity of network traffic [31]. Data centers globally handle an estimated 100 zettabytes of content yearly, and in this day and age, an individual user creates terabytes of data yearly, meaning that the amount of information crossing networks is astonishing [32]. To make sense of this deluge of information, sophisticated methods, such as data reduction, aggregation, and selective sampling, are required. The likelihood of missing valuable insights also increases

as more data becomes available. As more and more people use streaming services, cloud technology, and IoT devices, the diversity of network interactions increases, necessitating the analysis of both real-time and past events [33].

A new level of complication is being added by the shift to encrypted transmission. Google has reported that the percentage of encrypted web traffic on the internet increased from approximately 50 percent in 2014 to around 95 percent after 2020 [34], demonstrating how widespread the use of encryption has become in response to growing security concerns. Although encryption improves data privacy and security, it also hides packet contents, making deciphering them as difficult as deciphering coded letters. To break through the encryption wall and get intelligence without breaching data protection regulations, advanced methods like deep packet inspection (DPI) are required. DPI is widely recognized as a prominent contender in the field of web security, exhibiting considerable capabilities in effectively countering modern web-based threats. It is a process that involves examining the contents of packets as they traverse a specific location and afterward making instantaneous determinations based on predefined criteria established by the respective entity, such as the company, ISP, or network administrator [35]. Despite the recent advances in segregating the building blocks of network traffic in an attempt to tackle them independently, the NTMA community still has great trouble striking a balance between security and transparency, especially with the usage of decryption and user anonymity. Likewise, with an expected 41.6 billion devices—including mobile phones, tablets and IoT sensors—expected by 2025 as forecasted by IDC [36], it is becoming more difficult to standardize analytic procedures across devices and communication protocols. This necessitates the development of methods that can handle the nuances of multimodal traffic.

## 1.1.6 Use Cases of NTMA

The protection of vital digital assets is NTMA's top priority as the threat environment shifts and assaults become more sophisticated. To detect security breaches or malicious actions, NTMA analyzes network traffic patterns for deviations. The company Cybersecurity Ventures estimates that yearly expenditures related to cybercrime will amount to $10.5 trillion by 2025, making constant monitoring a crucial line of defense [37]. Network security experts may use NTMA's findings to strengthen protections, identify breaches, and react swiftly to new threats like distributed denial of service (DDoS) assaults and ransomware penetration [38].

When it comes to network optimization, which is crucial in today's digital economy where constant connection and fast data transfer are paramount, NTMA examines network traffic patterns to identify hotspots for congestion, as well as limitations in bandwidth and performance [39]. From this vantage point, IT managers can more effectively distribute network assets, enhance users' quality of service (QoS), and prevent service disruptions. With Ericsson predicting that 5G networks will reach 45 percent of the world's population by 2024, it is clear that effective network management is essential to satisfy consumer expectations as the market for fast and low-latency internet connectivity continues to rise [40].

Users may expect a flawless online experience thanks to NTMA's effective supervision of performance bottlenecks and optimization of network resources. This is evident in customer behavior where those who encounter website performance difficulties are less inclined to return to the site. Users' digital engagements are significantly impacted by NTMA's role in ensuring network flexibility and effectiveness, whether they are downloading high-definition material, holding virtual meetings, or making real-time online transactions [41].

More of NTMA's use cases are highlighted as follows:

- Network traffic characterization and monitoring
- Network optimization and planning
- Detection of network security violations
- Evaluation and improvement of network QoS
- Predictive maintenance of network components
- Forensic analysis
- Compliance and regulatory reporting
- Vulnerability scanning and patch management
- Cost optimization

### 1.1.7 Emerging Trends in NTMA

The incorporation of AI and ML into NTMA has been identified as a game-changing development. Artificial intelligence–driven insights offer important foresight about network activity in light of the daily data deluge. Companies like Cloudflare use AI to analyze massive volumes of network traffic data to identify and mitigate distributed denial of service (DDoS) attacks in real time. With the ever-increasing computational power at their disposal, NTMA is now able to not only spot patterns and abnormalities, but also predict them, in turn greatly improving network security and performance.

Edge computing's rise is also influencing changes to NTMA's methodology. NTMA has evolved from centralized evaluation to real-time monitoring as more and more IoT devices collect data at the network's edge. Pioneers of edge computing like Siemens use it in production, where material gathered from sensors implanted in equipment is evaluated locally for instantaneous decision-making [42]. This development allows NTMA to quickly detect problems and enhance performance as data is created, which helps to lessen delays and guarantee smooth user experiences.

In addition, the growing popularity of cloud computing is dramatically improving NTMA's versatility and accessibility [43]. Network operators now have the flexibility to install and administer remote monitoring throughout scattered environments with the help of cloud-based NTMA services like those provided by ThousandEyes, which is now part of Cisco [44]. This adaptability serves the ever-changing nature of network topologies, including the popularity of telecommuting. The move to NTMA in the cloud is an example of how the modularity and remote availability of the cloud meet the ever-changing needs of today's networks. These developments work together to provide NTMA with new capabilities, allowing it to flourish in the age of big data and digital complexity. NTMA plots a trajectory toward dynamic, smart, and proactive network management by making use of AI and ML, adopting edge computing, and integrating cloud solutions. Changes like this highlight NTMA's lasting impact on the reliable, high-performance networks that power the modern digital world [45].

### 1.1.8 Bridging the Gap between NTMA and User Experience

NTMA has emerged as the foundation of network responsiveness, durability, and ultimately user experience as the digital age has progressed. NTMA and the quality of experience (QoE) of the end user are intrinsically linked [46]. The capacity of NTMA

to analyze network traffic, pinpoint processing delays, and enhance QoS immediately translates into improved customer experience. Consider the case of a streaming platform that is monitored in real time with NTMA. Service monitoring and management teams can keep tabs on the status of the network and act quickly if there is a drop in streaming quality, which is often summarized as a mean opinion score (MOS) obtained through video quality assessment (VQA). This instantaneous adaptation goes hand in hand with viewers' evolving habits. For example, Netflix reported an increase of 15.77 million new subscribers in the first quarter of 2020, an increase of 23 percent over the same period in 2019 [47]. NTMA aids in client satisfaction and retention by guaranteeing a problem-free streaming experience.

In addition, NTMA's expertise applies to e-commerce, where customers' interactions have a major impact on their final purchases. The effectiveness of the network is crucial in the current environment. Potential latency concerns are identified by NTMA's study of user interactions and transaction flows, guaranteeing lightning-fast, error-free exchanges. Given that Statista predicts that global e-commerce sales will hit $5.56 trillion by 2027 [48], this is of utmost importance. Beyond its role in technical management, NTMA also helps drive revenue by improving the quality of the user experience.

Additionally, remote work scenarios benefit from the integration of NTMA and user experience. The rising popularity of working from home has made network speed and reliability more important than ever. Because of NTMA's efforts to reduce lag time, improve the quality of video conferences, and guarantee the timely transmission of data, dispersed teams can work together effectively. An overwhelming majority of remote workers, amounting to 58 percent, agree that telecommuting will increase in popularity over the next decade, as per research conducted by Owl Labs [49]. Due to the growing popularity of telecommuting, NTMA must prioritize QoE of streaming and video conference applications. To put it simply, NTMA bridges the gap between the technology economy and human experience. Improved user experience, engagement, and productivity are all direct products of NTMA's ability to analyze network dynamics and uphold performance.

## 1.2 Overview of Video Quality Assessment

The quality of video material has become a major differentiator in the complex digital fabric of contemporary multimedia consumption. Beyond the domain of basic technical standards, video quality assessment (VQA) stands as a key field that tries to objectively quantify and subjectively comprehend the perceptual quality of video output. VQA is, at

its core, an interdisciplinary field that draws from engineering, psychology, and human–computer interaction. The ultimate objective is to level the playing field between the technical aspects of video, such as resolution, bit rate, and compression artifacts, and the subjectivity of human viewers. This effort recognizes the intricacies of the human visual system, which include the interaction of cognitive processes, visual acuity, and psychological aspects that all contribute to the unique ways in which people take in and make sense of the world around them [50]. The rapid spread of streaming video across several channels highlights the need for VQA. It is crucial that the videos people watch online not only work technically but also captivate and immerse them. In this sense, VQA is the map that helps content producers, streaming services, and telecoms meet consumers where they want them to be in terms of the quality of the experiences they get.

Changes in the digital world have led to corresponding shifts in the variables that determine video quality. While extremely important, video quality factors like resolution and bit rate are only a small piece of the issue. Many elements can affect how an audience perceives a video, including compression artifacts, color correctness, motion fluidity, and audio synchronization. Thus, VQA incorporates both objective and subjective evaluation approaches, with the goals of measuring technical features and recording viewers' emotional responses.

The dynamic development of VQA may be seen in the shift from elementary, rule-based algorithms to sophisticated ML models. ML approaches may now be used to replicate human perceptual judgments, replacing older methods based on measures such as peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM). In recent years, deep learning architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have become extremely useful tools for gleaning subtle but important visual details from video [51].

In addition to its use in the entertainment industry, VQA has practical implications in the medical, security, and academic sectors. In medical imaging, for instance, an incorrect representation of diagnostic images might have fatal consequences. VQA reduces the potential for misunderstanding by making sure that medical images are true to their origins. With VQA, security professionals can be certain that they are viewing authentic, unedited video feeds, which assists in the discovery of abnormalities. VQA's continued exploration of AI, ML, and the psychology of perception has made it a centerpiece of the modern digital experience. It solidifies its role as a medium for providing not only videos, but also immersive visual tales that capture, connect, and reverberate with users by aligning technical requirements with human perception.

### 1.2.1 Significance of VQA

With video content sitting at the throne of current multimedia consumption trends, VQA is the heart that brings together content development and distribution strategies by molding user experiences through optimized metrics. VQA aims to answer questions such as how much of an impact video content quality has on audience engagement and satisfaction. Content-making industries such as internet protocol television (IPTV) broadcasters and over-the-top (OTT) streaming platforms require robust monitoring programs that display the current status of media being transmitted with regard to availability, running time, service quality, and user experience, which all form part of their feedback loop. This industry understands that viewers don't simply consume content; they live it. This section looks into the critical importance of VQA in today's multimedia ecosystem.

The direct effect of VQA on user engagement is likely the clearest indicator of its importance. The quality of the video content is the first line of interaction for digital customers in an age of abundant choices and short attention spans. This highly resonates with the thumping rise of short and captivating video consumption, among examples such as TikTok, YouTube Shorts, and Instagram Reels [52]. VQA operates as a watchdog, checking videos for flaws that might cause the viewer to be taken out of the experience, such as distortions, glitches, and other deficiencies. VQA ensures that videos have no distracting flaws, setting the stage for instant audience engagement. Among the advantages of VQA are its monetary effects. According to the *Harvard Business Review*, a 25 percent to 95 percent boost in profitability may be achieved by retaining just 5 percent more customers, leading to a direct correlation between content quality and viewer happiness [53].

The relevance of VQA goes beyond technical prowess to the psychological resonance of video. Videos are a powerful medium for sharing ideas, feelings, and experiences. VQA works to maintain the emotional resonance that gives videos their power, whether they are uplifting commercials, informative tutorials, or riveting narratives. Users have increasing expectations for video quality due to the proliferation of high-definition monitors, augmented reality, and virtual reality. User-created videos and live streaming have helped to democratize content creation, but this has led to a corresponding need to democratize quality. VQA's duty also includes analyzing content from many publishers to guarantee a constant, high-quality visual experience independent of the video's original source. Its relevance is far reaching and affects not just user engagement but also content developers and producers. VQA protects interest, financial gain, and emotional