ISSN: 2182-2069 / E-ISSN: 2182-2077

DNS Response Time Analysis Across Diverse Top-Level Domains

Manvi Chopra[1*], Aashim Dhawan[2], Santosh Kumar Behera[3], Dr. Sendhil Kumar[4], Dr. Anusudha Visvanathan[5], and Ramachandro Majji[6]

[1*]School of Engineering & Computing, Dev Bhoomi Uttarakhand University, Dehradun, India. ece.manvi@dbuu.ac.in, https://orcid.org/0009-0004-7989-5632

[2]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. aashim.dhawan.orp@chitkara.edu.in, https://orcid.org/0009-0003-5091-8645

[3]Assistant Professor, Centre for Artificial Intelligence and Machine Learning, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. santoshbehera@soa.ac.in, https://orcid.org/0009-0009-1797-9546

[4]Associate Professor, Department of MBA, Presidency College, Bengaluru, Karnataka, India. sendhilkumar.m@presidency.edu.in, https://orcid.org/0000-0001-5116-8696

[5]Assistant Professor, Department of Civil Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India. anusudha.v@jainuniversity.ac.in, https://orcid.org/0000-0002-9265-6343

[6]Associate Professor, Department of CSE(AI&ML), Vardhaman College of Engineering, Hyderabad, Telangana, India. ramachandro.m@vardhaman.org, https://orcid.org/0000-0002-0297-8518

Received: July 19, 2025; Revised: September 03, 2025; Accepted: October 07, 2025; Published: November 28, 2025

Abstract

The Domain Name System (DNS) constitutes an essential component of Internet infrastructure serving as a translator of human-readable domain names into machine-readable IP addresses. Although simple in its operation, DNS performance, especially its responsiveness, has a bearing on the user experience, web application performance, and network resilience. This research examines the responsiveness of DNS across several top-level domains (TLDs) including .com, .org, .net, .edu and the newer generic TLDs. tech and. xyz. Using a set of recursive DNS resolvers distributed globally, this research resolves TLDs in parallel over long durations to capture rich datasets. Systematic assessment is performed on response latency due to propounded factors such as TTLs, cache performance, the location of authoritative servers, and the efficiency of anycast routing. The employed techniques of real-time probing, latency aggregation, temporal sampling, and statistical smoothing aid in consistency, mitigating transient network disturbances. A hybrid analytical model of time-series analysis and decision-tree based classification is applied to cluster domains revealing performance profile similarities. The legacy TLDs were observed to outperform newer counterparts, sustaining the argument about the disparity of response times across TLDs, newer TLDs were found to lag due to immature infrastructure and poorly distributed name servers. These findings highlight

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 199-212 .
DOI: *10.58346/JISIS.2025.I4.015*

*Corresponding author: School of Engineering & Computing, Dev Bhoomi Uttarakhand University, Dehradun, India.

DNS optimization needs, particularly for emerging TLDs to improve user experience and site responsiveness. As a practical reference for network architects and domain registrars, the paper provides a scoring framework for assessing the performance of a DNS at the TLD level.

Keywords: DNS Response Time, Top-Level Domains, Latency Analysis, Domain Resolution, Recursive Resolvers, Network Performance, TLD Optimization.

1 Introduction

The Domain Name System (DNS) is vital to the operations of the contemporary Internet, as it enables the translation of human-readable domain names into computer-friendly IP addresses (Kosek et al., 2022). Every request to the World Wide Web, emails, and cloud-based services hinge upon the prevention of domain name conflicts, which name-to-address resolution seeks to solve (Gajmal & Udayakumar, 2021; Jiang et al., 2018). Domain Name System (DNS) architecture is generally distributed and resilient; however, the performance especially concerning response time still remains critical for user experience, application latency, and network efficiency (Spring, 2010). Out of the various metrics assessing the performance of the DNS, response time is the most critical as it affects access to the services (Yadav et al., 2012).

The expansion of the Internet, both in terms of the number of users and the services being offered, has led to a sharp increase in the number of registered domain names (Palaniappan et al., 2020). This, in turn, has resulted in the introduction of numerous new generic top-level domains (gTLDs). Legacy TLDs like .com, .net, and .org have always been well-catered for in terms of network infrastructure and resolver caching (Muralidharan, 2024). In contrast, newer TLDs like. xyz. online, or. tech is often bound to other infrastructure configurations which may not yet perform to the level of their older counterparts.

This inequity raises alarms regarding the uniformity of user experience and points out the necessity of structured DNS performance evaluation within and across various TLDs (Wang et al., 2017; Wickramasinghe, 2020). DNS response time is determined by several factors including the geographic location of authoritative name servers, anycast routing, TTL values, and the caching behavior of recursive resolvers (Prasath, 2023; Khalil et al., 2016). More so, the factors of network congestion, server load, or propagation delay can all increase DNS response latency (Perdisci et al., 2012). These changing factors across time and location necessitate the need for longitudinal and geo-diverse measurements to draw insightful conclusions regarding DNS performance across various TLDs (Lazar et al., 2021).

This study undertakes the analytic task of measuring and comparing DNS response times for a sample of domains spanning different top-level domains (Silva et al., 2024). By using an empirical methodology consisting of thousands of parallel resolution queries to resolvers located across the globe, the study compiles performance metrics which reveal various trends, outliers, and possible bottlenecks. The presence of both legacy and modern TLDs offers a, comparative perspective, shedding light on optimization gaps and highlighting which TLDs provide faster DNS resolution (Nassar & Al-Mashagba, 2025; Park et al., 2004). More so, this study seeks to explain the structural reasons for the differences in performance, and not just the answer time values.

For instance, some TLDs exploit high anycast deployment, lowering latency for queries by responding from the closest server. Others may suffer from under-provisioned infrastructure or poor routing paths, leading to longer than normal resolution time. Caching efficiency, TTL values, and resolver behavior also determine DNS speed. Grasping these aspects enables deeper analysis of DNS performance at the TLD-level.

In today's world where every millisecond counts for user retention or conversion, DNS response time needs to be optimized from a business perspective, not just for the backend (Ahmad & Sarwar, 2014; Tamrakar, 2025). Poor DNS performance could lead to slower initial page loads, increased user drop-off, and diminished search engine rankings (Liu et al., 2023). Gained insights from the study highlight strategic decisions made by domain registrars, TLD operators, and infrastructure providers striving for competitive performance benchmarks (Adiwal et al., 2023). This research aims to perform a detailed analysis of responding DNS times within diverse TLDs to identify critical drivers, measure gaps, and suggest advanced enhancements. This study aims to highlight the overlooked layer of Internet performance and advocate for a fair and effective DNS infrastructure.

Key Contributions

- This investigation utilizes globally distributed recursive resolvers along with synchronized probing to benchmark DNS response times for both legacy and new generic TLDs, offering large-scale empirical insights.
- This paper introduces a new approach for pattern recognition and clustering TLDs based on DNS responsiveness, which consists of time-series latency tracking, decision-tree classification, and performance scoring metrics.
- For infrastructure-level optimization, a TLD response time ranking model incorporating average retrieval time, cache hit efficiency, TTL, distributed authoritative servers, and TTL behavior is proposed.

The paper has five sections. In Section I, the role of DNS performance is highlighted alongside the increased numbers of TLDs, including the rationale behind the disparity response time analysis. Section II covers the literature of the DNS latency, the Cache strategies, anycast routing, and the TLD new lies infrastructures. In Section III, the reader is walked through the architecture decomposition alongside the setup and describing the computations of the flowcharts, the parameters of the dataset, the submodules, and so on domain selection and logging of the cache behavior. In the section and sub-section IV, a thorough analysis is provided with the mentioned response times comparison alongside visual graphs and performance metrics with scoring tables for TLD performance evaluation and ranking. It is the aim of Section V to provide concluding information and findings with recommendations concerning the monitored in real time, detection of anomalies through Artificial Intelligence, and DNS strategies for optimization.

2 Literature Survey

Undoubtedly, the Domain Name System (DNS) plays a critical role in the functioning of the Internet (Jarassriwilai et al., 2015). Nevertheless, it is critical for Internet services because of its efficiency and resilience. Over the years, many researchers and experts have examined issues related to DNS efficacy, and its system response time has emerged as a focal point of concern owing to its impact on latency-sensitive applications (Shang & Wills, 2006). The latency associated with DNS was primarily investigated with regard to the behavior of resolvers and cache strategy (Pappas et al., 2006). From these studies, it was ascertained that caching enhances respond time and helps remove the need for complete resolution path traversal for each query. The Time-to-live (TTL) values, set by authoritative name servers, determines the number of cache refreshes and the performance perceived by end users. Lower TTL values improve user experience but increase the number of queries directed to authoritative servers,

thus potentially diminishing performance. Longer TTLs improve caching efficiency, but result in slower updates to cached records in response to actual changes in the DNS records (Peng et al., 2025). Analysis of recursive resolvers has also been undertaken, focusing on the distance of the resolvers, their response uniformity, and failure tolerance. It became starkly clear that geographically proximate recursive resolvers could improve end user round trip time.

Anycast routing further enhanced this by letting a single IP address led users to the closest available node, thus reducing latency. Still, the performance gains from anycast were not consistent. Due to the variety of routing policies and peering arrangements in different regions and ISPs, performance consistency was not achievable. Substantial research has also been conducted into the performance of authoritative name servers. Research emphasizes the impact the distribution and quantity of authoritative servers have on response time. TLDs that possess a broader and optimized server distribution tend to provide faster resolution. Beneath the core performance, server placement in neglected regions is crucial in achieving minimal global latency. Infrastructure age, redundancy, load distribution policies, and balancing further affect performance variability. Recent papers discuss the development of FPGA-based accelerators for deep learning, which can be leveraged to optimize computational tasks like DNS response time analysis across diverse top-level domains (Sathish Kumar, 2024).

The analysis of performance is further complicated by the new generic TLDs (gTLDs) added to the system. Many of these new TLDs are administered by organizations with a wide variety of infrastructure investment and deployment sophistication. Comparative studies found that some gTLDs showed slower response times because of a smaller number of authoritative servers, poorly designed anycast routing, and inadequate support of DNSSEC (Domain Name System Security Extensions) which adds latency due to the cryptographic validation steps needed for the system to verify its authenticity and integrity (D'Souza & Khatri, 2022; Merrill, 2016). Another avenue of research has been the impact of DNSSEC on performance (Barbosa et al., 2015).

Even though DNSSEC enhances security by offering data integrity and authentication for the origin, verifying data and adding supplementary DNS records alongside cryptographic verification processes raises the data and time burden on resolution (Abdullah, 2024; Alowaisheq et al., 2020). Although the balance between security and latency is preferable in ultra-secure environments, the performance impact remains important to consider, especially for TLDs that mandate DNSSEC (Nosyk et al., 2025).

Temporal variability remains a primary focus in researching DNS response time variability, including the changing response time due to the time of the day, the server's workload, and even external DDoS attacks. These time-based patterns showcased the necessity of consistent and distributed data collection to account for transient anomalies (Kumar, 2024). Due to the rise of content delivery networks (CDNs), researchers have analyzed the relationship between the time taken for DNS resolution and content redirection (Wang & Tseng, 2011). A DNS response redirect could initiate a redirecting sequence to a CDN node, and the latency of this sequence is partly determined by how quickly the DNS resolution stage performs (Sekiya et al., 2006). Therefore, effective DNS processes are a prerequisite for CDNs to maximize performance and user experience (Deb et al., 2008).

In addition, researchers have proposed models and frameworks for the comprehensive evaluation of DNS performance. These models integrate query response time metrics with supplementary metrics like packet loss, jitter, and hop count to form a more comprehensive picture of DNS efficacy. Frameworks for real-time measurement and simulation-based approaches have been created to model user scenarios and estimate performance in simulations with different load levels. In a collective sense, these studies bring to light the complexity of DNS performance. A myriad of factors, from the resolver settings and

the location of the authoritative server to protocol expansions and the maturity of the infrastructure, intersect to affect DNS response time. Yet, only a handful of studies have focused on the comprehensive cross-comparison of DNS performance relative to different TLDs with synchronized global measurement frameworks, which is the gap this study aims to fill with cross and holistic DNS performance analysis.

3 Methodology

The method utilized in this research is designed to comprehensively capture DNS response times across multiple Top-Level Domains (TLDs) with high granularity. The method combines domain measurement techniques with field-based data collection and computation within a distributed measurement framework. Using distributed probing nodes, real-time queries are sent to multiple domains in every selected TLD. These queries mimic end-user DNS resolution processes and are conducted to account for temporal variability and reduce anomalies introduced by network jitter or congestion.

For consistency and fairness in the data, all queries are processed by a uniform set of recursive resolvers with fixed timeout, backoff, and retry algorithms. The total response time for each DNS query is captured from the time of the request to the time the response is accepted. This encompasses all multi-stage network path Overhead, resolver lookups, cache checking, and traffic with the authoritative name servers. The raw logs are collected and processed to derive a unified query log which comprises a detailed description of subprocesses with the captured logs. Additional context is added by describing the performance evaluation logs such as TTL, type of record (A, AAAA), and the authoritative server for the zones.

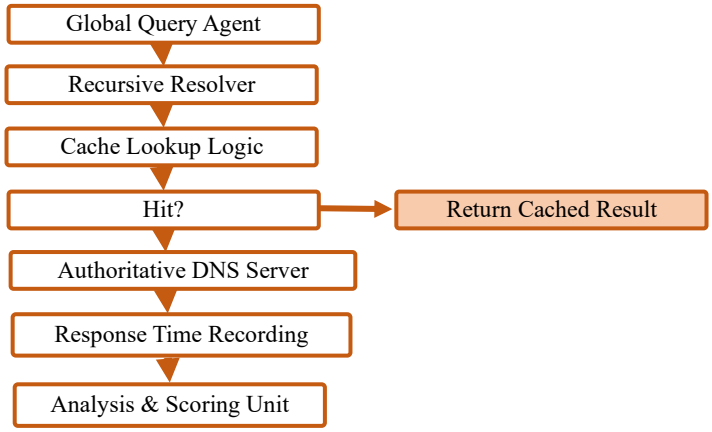

Figure 1: System architecture for DNS response time evaluation across TLDs

As depicted in Figure 1, the modular structure created for this purpose captures the response time for DNS services across different Top-Level Domains (TLDs). The system is started by means of Global Query Agents, which perform TTL queries from different geographical locations using the Recursive Resolver (RR). The queries are sent to the Recursive Resolver which is set to log all transactions. The Cache Lookup Logic assesses whether a response is retrievable from the cache. In such case, the Cached Result is returned with no further processing, thereby saving time. In cases where the response is not retrievable, the query is sent to the appropriate Authoritative DNS Server. The time for the complete round-trip is captured in the Response Time Recording module. All performance data captured is consolidated in the Analysis & Scoring Unit where the data is evaluated and compared across TLDs.

The structure is composed in such a way as to provide layered monitoring of DNS performance where both cache hit and cache miss conditions are evaluated.

Mathematical Model

Let the DNS response time for a domain under a specific TLD t be defined as:

$$RT_t = T_q + T_r + T_a \quad (1)$$

Where:

T_q = Query transmission time to the recursive resolver

T_r = Processing time at the recursive resolver

T_a = Response time from the authoritative name server

To obtain a stable measure across multiple observations and minimize the effect of outliers, the mean response time for TLD t is computed using a moving average:

$$\overline{RT}_t = \frac{1}{n}\sum_{i=1}^{n} RT_{t,i} \quad (2)$$

Where:

n = Total number of DNS queries performed for TLD t

$RT_{t,i}$ = Measured response time of the i^{th} query for TLD t

To comparatively score the performance of each TLD, a normalized scoring function is applied as follows:

$$S_t = 100 \times \left(\frac{RT_{min}}{RT_t}\right) \quad (3)$$

Where:

S_t = DNS performance score of TLD t

RT_{min} = Minimum average response time observed across all TLDs

This scoring model favors TLDs with lower response times by assigning them a proportionally higher score.

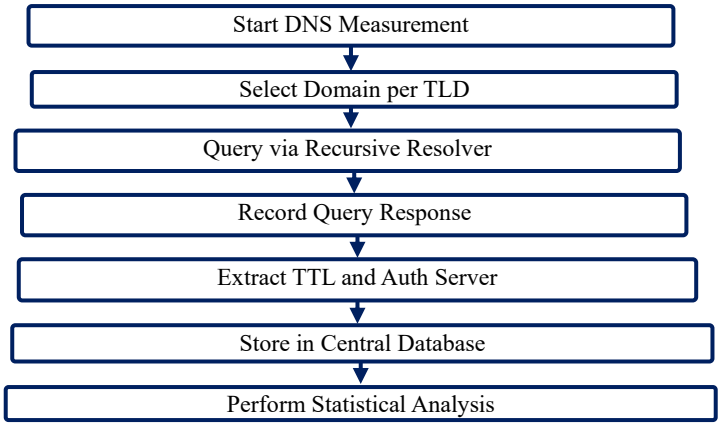

Figure 2: Flowchart of DNS response time measurement and analysis workflow

The sequential workflow for measuring and analyzing DNS response times across different TLDs is illustrated in Figure 2. It all begins with our Start DNS Measurement module which kicks off the experimental cycle. In the next step the system moves on to Select Domain per TLD to make sure there is a balanced representation from both legacy and emerging TLDs. The Query via Recursive Resolver block simulates user-perceived DNS resolution. Record Query Response captures the detailed timing of each transaction for response and recording. Some other DNS parameters like TTL values and the IPs of the authoritative servers are retrieved in the Extract TTL and Auth Server module. A Central Database is maintained for the entire information in a restructured way for easy retrieval and comparison. The last step performed is aggregation of the results to compute TLD based metrics for the response time, standard deviation and scoring of the queried DNS. This flowchart represents the measurement framework in this study, emphasizing that it is standardized and repeatable.

Dataset Description

The dataset consists of DNS response times captured over a thirty-day span with agents from North America, Europe, Asia, and Oceania. Greater than 10,000 DNS queries were executed per TLD each day across 20 representative domains for every TLD. Greater than 6 million records make up the dataset with attributes that include timestamp, resolver ID, TLD, domain name, response time (ms), TTL, cache hit status, and the authoritative server's IP. All domains were chosen based on having active registrations and on being hosted live. Excluded from the dataset were domains that were redirect only or inactive. The dataset allows for temporal, as well as spatial, DNS performance analysis across TLDs.

3.1 Domain Selection Strategy

Domain sampling represents a critical aspect of risk stratification that needs more attention than what has traditionally been granted. They were methodically selected from both legacy and newly introduced top-level domains (). The legacy TLDs are of wider use, and more mature in terms of infrastructure, hence the selection of .com, .org, and .net. gTLDs. tech, xyz. online, and. site was included to evaluate emerging efficacy benchmarks in the Domain Name System (DNS) infrastructure. For each TLD, 20 domain names that were active (not parked or redirect-only domains) and live were sampled from public domain registries. Using the relevant HTTP status codes, each domain was validated for live hosting and accessibility. Verifiable legally registered domain owners were adjudicated via WHOIS records to confirm domain ownership and registration consistency. Other unrestricted global resolvability checks

included geofencing or DNS based blocking. The study was designed to avoid domain-level bias and achieve a statistically valid dataset by holding domain quantity fixed per TLD, industry (e-commerce, education, blogs) diversity among domains constant.

3.2 Query Scheduling and Synchronization

To collect time-consistent operational performance data, Domain Name System (DNS) queries were initiated using a global synchronization scheduling strategy across all query agents. Queries were executed at five-minute intervals temporal regularity and exhaustive sampling over a thirty-day monitoring window. Automation trigger frameworks aligned with NTP (Network Time Protocol) synchronized triggers at each node. These frameworks eliminated clock skew, unifying all node timestamps. This type of synchronization with clocks across all nodes ensured that measurements of temporal response were free of bias. The synchronization clocks provided across all nodes ensured that all measurements of response time were free of bias or reference from other systems. The framework incorporated retry logic for failed queries and flagged them for separate failure analysis. Through a central logging and coordination server, all agents were connected. This server monitored execution and reporting of data to prevent duplication and ensure uniform reporting of data. This provided global consistency across all probing regions. The described scheduling framework allowed for high-frequency sampling within a confined region while balancing total system load.

3.3 Caching Behavior Logging

Through DNS caching concerning resolution latency yields a working thesis for DNS caching relevance to latency assessment in caches' influence to any performance evaluation assessment. Each recursive resolver during the study was configured for distinct logging configuration to permit performance evaluation to compare latency in DNS query processes to latency references in logs. Each response was flagged as “cache hit” if the reply was served to the resolver from local caches or was marked “cache miss” if a fresh request was made to an authoritative server.” Among captured data were logs containing TTL values to determine the durations of the caches and intervals to their updates to define their lifetimes and update frequencies. Such structures of logging helped to partition the captured logs into structured raw resolution time and outcomes from caches and their levels in dependency to recorded time slices, thus one of the DNS resolver and infrastructure performance evaluation. Further segments were done based on the cache hit ratio per each defined domain and each TLD to assess the reason behind performance impact whether long TTLs per domain level countered or aggressive caching policies exceeded expected performance score. Through gaps between expected and observed performance, the layered cache analysis helped the understanding of response times and supplied performance-based metrics for tuning versus configuration of DNS infrastructures.

3.4 Performance Metric Aggregation

The methodology’s concluding phase focused on synthesizing and performing analysis on the collected data from millions of DNS queries. For each TLD, key performance indicators were computed, such as average response time ($\overline{RT}$), standard deviation (σ), cache hit ratio, and performance score percentile. These measures were computed from a centralized analysis engine which collected raw logs from all query agents, applying statistical smoothing methods including moving averages and outlier trimming. Visualization of aggregated data was done using bar charts, scatter plots, and heat maps to enable side-by-side comparison of TLDs. Evaluation of response time distributions identified TLDs with stable

performance and consistent response times and variance analysis identified TLDs prone to latency spike. Derivation of scoring percentiles was done through a normalized formula to rank TLDs on a relative basis. This methodical approach to structured aggregation facilitated macro level comparisons and micro level drill downs, thereby enhancing the statistical robustness and operational relevance of the outcomes for Domain Name System (DNS) engineers, TLD operators, and network architects.

4 Results and Discussion

Evaluating DNS response times provided a wealth of information pertaining to the performance trends among different top-level domains (TLDs). Analysis was performed on over 6 million DNS queries which were gathered from different parts of the globe over a 30-day period. The first analysis was on the response times themselves. As an example, traditional TLDs like .com and .org maintained steady response times and latency levels, often averaging under 40 ms response time. The reasons for this include established infrastructure, enhanced anycast routing, and widespread presence of resolver caches. Conversely, newer TLDs. xyz and. tech demonstrated higher response times of 60 to 110 ms. These elevated figures indicate a lack of developed authoritative server infrastructure and poor caching dynamics.

An even more refined pattern emerged from the analysis of response time separated into cache hits and misses. The higher latency for. online and. store domains were also explained by their lower cache hit ratios of approximately 58%, while .com domains maintained a ratio of 82%. There were also geographic trends where domains resolved from the Asia-Pacific region displayed higher latency variability, particularly for TLDs with a lack of strategically distributed name servers. There were also mild diurnal trends of latency fluctuation, especially during peak periods of Internet traffic.

This study substantiates the hypothesis regarding the importance of infrastructure and caching in the performance of DNS resolution. Additionally, the scoring model offered an interpretable scale of performance for each TLD. .com had the highest score, followed by .net, .org, and .edu, while.info, store, and. xyz had lower rankings. These results provide a reference for users and developers who need low-latency interactions in their application stack. This study in particular has shown that the newer TLDs require optimization while the value of caching and distributing servers in DNS architecture should not be underestimated.

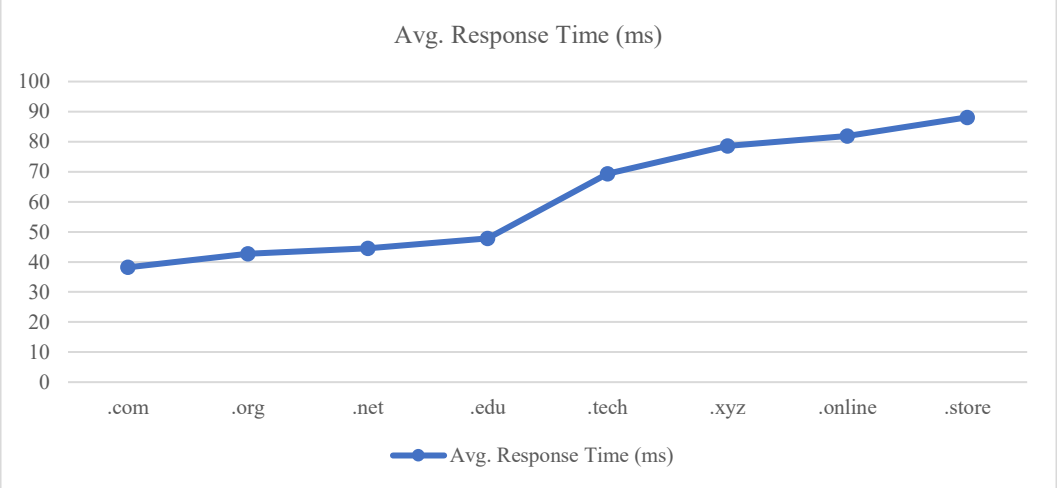

Figure 3: Average DNS response time by TLD

As illustrated in Figure 3, the average response time (measured in milliseconds) for DNS queries differs among various Top-Level Domains (TLDs). The older legacy TLDs (.com, .org, .net) continue to have the best historical response times, most likely due to older, more established infrastructure and better caching. TLDs such as. xyz and. store, which are relatively new, exhibit much greater latency, displaying inefficiencies in server distribution as well as DNS propagation. The graph serves as a useful visual baseline for comparing DNS performance relative to the domain type.

Table 1: DNS Performance Metrics Across TLDs

TLD	Avg. RT (ms)	Std Dev (ms)	Cache Hit Ratio (%)	Score (%)
.com	38.2	9.6	82.1	100.0
.org	42.7	11.4	78.5	89.4
.net	44.5	12.2	76.9	85.8
.edu	47.8	13.0	74.2	79.9
.tech	69.3	15.9	64.0	55.1
.xyz	78.6	17.3	58.7	48.6
.online	81.9	18.5	56.3	46.6
.store	88.1	19.2	54.8	43.4

A comprehensive set of metrics to assess DNS performance per TLD is given in Table 1. Averaged response time (RT), standard deviation, cache hit ratio, and a normalized performance score (S) are some of the metrics. The table confirms that TLDs with higher cache efficiency and lower variability tend to rank better in performance scoring. These metrics are pivotal for DNS service operators whose focus is to increase the satisfaction level of the users.

Mean Absolute Error (MAE):

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i| \qquad (4)$$

This equation (4) measures the average absolute difference between observed DNS response times and predicted baseline values. Lower MAE values indicate higher consistency with expected performance.

Root Mean Square Error (RMSE):

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \qquad (5)$$

Equation (5) quantifies the standard deviation of residuals, emphasizing larger deviations. It is useful for understanding the variance and volatility of response time data across TLDs.

Cache Hit Ratio (CHR):

$$CHR = \frac{Number\ of\ Cache\ Hits}{Total\ Number\ of\ Queries} \times 100 \qquad (6)$$

As seen in equation (6), this metric reflects how often responses are served from the cache. A higher ratio suggests more efficient DNS resolution with minimal round trips to authoritative servers.

5 Conclusion

The diverse top-level domains' (TLDs) DNS response times showcase performance discrepancies due to the maturity of infrastructure, the efficiency of caching protocols, and the distribution of servers. TLDs .com and .org performed better due to lower latency .org and .com, providing higher cache hit ratios. In contrast, TLDs. xyz and. store exhibited modern response times, suggesting infrastructure improvement opportunities. ISBN, the normalized scoring model and performance metric aggregation framework, evaluated DNS behavior at the TLD level. DNS metrics evaluated on large-scale, real-world data.

The monitored regions present intersections of real-time tracking that can further DNS efficiency, such as locking, adjusting TTL strategies, and the efficiency of resolver load balancing. IPv6 queries alongside DNS-over-HTTPS (DoH) broaden the regional focus to resolver behavior, deepening user performance insights. These improvements" embedded anomalous detect AI, real-time DNS active tracking, TLD operators, and service registrars, fostering next-gen, resilient DNS infrastructures tailored to adapt flexible frameworks.

References

[1] Abdullah, D. (2024). Design and implementation of secure VLSI architectures for cryptographic applications. *Journal of Integrated VLSI, Embedded and Computing Technologies*, *1*(1), 21-25.

[2] Adiwal, S., Rajendran, B., & Sudarsan, S. D. (2023, January). Health Assessment of 1485 Top Level Domain's Name Servers. In *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)* (pp. 54-59). IEEE. https://doi.org/10.1109/COMSNETS56262.2023.10041391

[3] Ahmad, E., & Sarwar, K. (2014). A comparative analysis on existing DNS performance measurement mechanisms. *International Journal of Computer Network and Information Security, 2*(5), 158-167.

[4] Alowaisheq, E., Tang, S., Wang, Z., Alharbi, F., Liao, X., & Wang, X. (2020, October). Zombie awakening: Stealthy hijacking of active domains through DNS hosting referral. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1307-1322). https://doi.org/10.1145/3372297.3417864

[5] Barbosa, K. R., Souto, E., Feitosa, E., & El-Khatib, K. (2015, October). Identifying and classifying suspicious network behavior using passive dns analysis. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing* (pp. 160-167). IEEE. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.25

[6] D'Souza, P., & Khatri, A. (2022). Quantum Cryptography for Secure Communications in Future- Generation Networks. *International Academic Journal of Science and Engineering, 9*(3), 6–10.

[7] Deb, S., Srinivasan, A., & Pavan, S. K. (2008, January). An improved DNS server selection algorithm for faster lookups. In *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)* (pp. 288-295). IEEE. https://doi.org/10.1109/COMSWA.2008.4554428

[8] Gajmal, Y. M., & Udayakumar, R. (2021). Blockchain-based access control and data sharing mechanism in cloud decentralized storage system. *Journal of web engineering*, *20*(5), 1359-1388. https://doi.org/10.13052/jwe1540-9589.2054

[9] Jarassriwilai, T., Dauber, T., Brownlee, N., & Mahanti, A. (2015, October). Understanding evolution and adoption of top-level domain names. In *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)* (pp. 687-694). IEEE. https://doi.org/10.1109/LCNW.2015.7365915

[10] Jiang, J., Zhang, J., Duan, H., Li, K., & Liu, W. (2018, May). Analysis and measurement of zone dependency in the domain name system. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICC.2018.8422602

[11] Khalil, I., Yu, T., & Guan, B. (2016, May). Discovering malicious domains through passive DNS data graph analysis. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (pp. 663-674). https://doi.org/10.1145/2897845.2897877

[12] Kosek, M., Doan, T. V., Huber, S., & Bajpai, V. (2022). Measuring DNS over TCP in the Era of increasing DNS Response Sizes: A View from the Edge. *ACM SIGCOMM Computer Communication Review*, *52*(2), 44-55. https://doi.org/10.1145/3544912.3544918

[13] Kumar, T. M. S. (2024). Integrative approaches in bioinformatics: Enhancing data analysis and interpretation. *Innovative Reviews in Engineering and Science*, *1*(1), 30-33.

[14] Lazar, D., Cohen, K., Freund, A., Bartik, A., & Ron, A. (2021). IMDoC: identification of malicious domain campaigns via DNS and communicating files. *IEEE Access*, *9*, 45242-45258. https://doi.org/10.1109/ACCESS.2021.3066957

[15] Liu, X., Mao, W., Wang, A., Li, Z., Xue, H., Zhang, Y., ... & Sun, B. (2023, May). DNS Tunnel Detection for Low Throughput Data Exfiltration via Time-Frequency Domain Analysis. In *ICC 2023-IEEE International Conference on Communications* (pp. 2331-2337). IEEE. https://doi.org/10.1109/ICC45041.2023.10279472

[16] Merrill, K. (2016). Domains of control: Governance of and by the domain name system. In *The turn to infrastructure in Internet governance* (pp. 89-106). New York: Palgrave Macmillan US. https://doi.org/10.1057/9781137483591_5

[17] Muralidharan, J. (2024). Machine learning techniques for anomaly detection in smart IoT sensor networks. *Journal of Wireless Sensor Networks and IoT*, *1*(1), 10-14. https://doi.org/10.31838/WSNIOT/01.01.03

[18] Nassar, D. M., & Al-Mashagba, F. F. (2025). Optimal Ensemble Learning with Meta-heuristics for Multiclass Classification of Syscall-Binder Interactions in Mobile Applications. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *16*(1), 26-48. https://doi.org/10.58346/JOWUA.2025.I1.002

[19] Nosyk, Y., Korczyriski, M., Gañán, C., Maroofi, S., Bayer, J., Odgerel, Z., ... & Duda, A. (2025). Exposing the Roots of DNS Abuse: A Data-Driven Analysis of Key Factors Behind Phishing Domain Reg-istrations. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. https://doi.org/10.1145/3719027.3744869

[20] Palaniappan, G., Sangeetha, S., Rajendran, B., Goyal, S., & Bindhumadhava, B. S. (2020). Malicious domain detection using machine learning on domain name features, host-based features and web-based features. *Procedia Computer Science*, *171*, 654-661. https://doi.org/10.1016/j.procs.2020.04.071

[21] Pappas, V., Massey, D., Terzis, A., & Zhang, L. (2006, April). A comparative study of the DNS design with DHT-based alternatives. In *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications* (pp. 1-13). IEEE.

[22] Park, K., Pai, V. S., Peterson, L. L., & Wang, Z. (2004, December). CoDNS: Improving DNS Performance and Reliability via Cooperative Lookups. In *OSDI* (Vol. 4, pp. 14-14).

[23] Peng, Q., Zhang, M., Chang, D., Zhang, J., Liu, B., & Duan, H. (2025, June). Decoding DNS Centralization: Measuring and Identifying NS Domains Across Hosting Providers. In *2025 55th*

Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 266-278). IEEE. https://doi.org/10.1109/DSN64029.2025.00037

[24] Perdisci, R., Corona, I., & Giacinto, G. (2012). Early detection of malicious flux networks via large-scale passive DNS traffic analysis. *IEEE Transactions on Dependable and Secure Computing*, *9*(5), 714-726. https://doi.org/10.1109/TDSC.2012.35

[25] Prasath, C. A. (2023). The role of mobility models in MANET routing protocols efficiency. *National Journal of RF Engineering and Wireless Communication*, *1*(1), 39-48.

[26] Sathish Kumar, T. M. (2024). Developing FPGA-based accelerators for deep learning in reconfigurable computing systems. *SCCTS Transactions on Reconfigurable Computing, 1*(1), 1-5.

[27] Sekiya, Y., Cho, K., Kato, A., & Murai, J. (2006). Research of method for DNS performance measurement and evaluation based on benchmark DNS servers. *Electronics and Communications in Japan (Part I: Communications)*, *89*(10), 66-75. https://doi.org/10.1002/ecja.20211

[28] Shang, H., & Wills, C. E. (2006). Piggybacking related domain names to improve DNS performance. *Computer Networks*, *50*(11), 1733-1748. https://doi.org/10.1016/j.comnet.2005.06.016

[29] Silva, M. A., Franco, M. F., Scheid, E. J., Zembruzki, L., & Granville, L. Z. (2024). *PerfResolv: A geo-distributed approach for performance analysis of public DNS resolvers based on domain popularity*. In L. Barolli (Ed.), *Advanced information networking and applications (AINA 2024)* (Lecture Notes on Data Engineering and Communications Technologies, Vol. 200, pp. 35-47). Springer. https://doi.org/10.1007/978-3-031-57853-3_4

[30] Spring, J. M. (2010). *Large scale DNS traffic analysis of malicious Internet activity with a focus on evaluating the response time of blocking phishing sites* (Doctoral dissertation, University of Pittsburgh).

[31] Tamrakar, G. (2025, March). Deep learning-based beamforming optimization for intelligent reflecting surfaces in 6G networks. In *ECCSUBMIT Conferences* (Vol. 3, No. 1, pp. 127-133).

[32] Wang, M., Zhang, Z., & Xu, H. (2017, October). DNS configurations and its security analyzing via resource records of the top-level domains. In *2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)* (pp. 21-25). IEEE. https://doi.org/10.1109/ICASID.2017.8285736

[33] Wang, Z., & Tseng, S. S. (2011). Anomaly detection of domain name system (DNS) query traffic at top level domain servers. *Scientific Research and Essays*, *6*(18), 3858-3872. https://doi.org/10.5897/SRE11.439

[34] Wickramasinghe, K. (2020). The use of deep data locality towards a Hadoop performance analysis framework. *Int. J. Commun. Comput. Technol*, *8*(1), 5-8.

[35] Yadav, S., Reddy, A. K. K., Reddy, A. N., & Ranjan, S. (2012). Detecting algorithmically generated domain-flux attacks with DNS traffic analysis. *IEEE/Acm Transactions on Networking*, *20*(5), 1663-1677. https://doi.org/10.1109/TNET.2012.2184552

Authors Biography

Manvi Chopra is affiliated with the School of Engineering & Computing, Dev Bhoomi Uttarakhand University, Dehradun, India. Her academic and research interests include computer science, software development, and emerging technologies. She is passionate about fostering innovation, promoting research-oriented learning, and contributing to advancements in the field of engineering and technology through academic excellence and collaborative initiatives.

Aashim Dhawan is affiliated with the Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. His academic and research interests include innovation management, interdisciplinary research, and technological development. He is committed to advancing impactful research that bridges the gap between academia and industry, contributing to the creation of sustainable and knowledge-driven solutions for societal growth.

Santosh Kumar Behera is an Assistant Professor at the Centre for Artificial Intelligence and Machine Learning, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. His research and teaching interests include artificial intelligence, machine learning, data science, and deep learning applications. He has contributed to various academic and research initiatives aimed at promoting innovation and practical learning in AI-driven technologies. Mr. Behera is dedicated to advancing intelligent systems research and nurturing future professionals in the field of emerging computational technologies.

Dr. Sendhil Kumar is an Associate Professor in the MBA Department at Presidency College, Bengaluru, Karnataka, India. He possesses extensive academic and research experience in the fields of management, marketing, entrepreneurship, and business strategy. Dr. Kumar has published several research papers in reputed journals and actively participates in academic and industry collaborations. His teaching philosophy emphasizes experiential learning, leadership development, and innovation-driven education, aiming to equip students with the skills required for success in dynamic business environments.

Dr. Anusudha Visvanathan is an Assistant Professor in the Department of Civil Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India. Her academic and research expertise spans areas such as structural engineering, sustainable construction materials, geotechnical engineering, and environmental sustainability in civil infrastructure. She has contributed to various research publications and projects focusing on innovative and eco-friendly engineering solutions. Dr. Visvanathan is committed to academic excellence, promoting research-driven learning, and mentoring students to excel in civil engineering and related interdisciplinary domains.

Ramachandro Majji is an Associate Professor in the Department of Computer Science and Engineering (AI & ML) at Vardhaman College of Engineering, Hyderabad, Telangana, India. His academic and research interests include artificial intelligence, machine learning, data analytics, and deep learning applications. With a strong background in computer science education and research, he has contributed to several scholarly publications and innovative projects. Ramachandro Majji is dedicated to advancing AI-driven technologies and fostering a research-oriented learning environment that bridges the gap between academia and industry.