PerfResolv: A Geo-Distributed Approach for Performance Analysis of Public DNS Resolvers Based on Domain Popularity

Marcelo Almeida Silva, Muriel Figueredo Franco, Eder John Scheid,
Luciano Zembruzki, Lisandro Zambenedetti Granville

Abstract The Domain Name System (DNS) represents one of the cornerstones of the World Wide Web and plays an indispensable role in its operation. DNS is an extensive distributed database structured to resolve readable domain names for people, companies, and institutions into corresponding and reliable IP addresses. This paper presents PerfResolv, an approach for performance analysis on public DNS resolver servers (e.g., Google, Cloudflare, OpenDNS, Quad9, and ComodoDNS). The analysis was performed with PerfResolv located at geographically distributed points in three different countries: Brazil, Switzerland, and Australia. The results were obtained considering the response time for resolving domain names with different popularity levels to verify if and how geolocation, domain name popularity, week, day, and time affect the performance of DNS resolver servers. The results show considerable fluctuations in the response time of some DNS resolvers, with a variation of up to 40% in response time across different hours of the day. Further, there are differences between the resolution time of popular and unpopular domains, which are also influenced by the geolocation of the measurement monitors.

1 Introduction

The Internet has become indispensable due to the importance of its applications and possibilities of use in different sectors of industry, government, and entertainment. The Domain Name System (DNS) represents one of the foundations of the Internet, playing an indispensable role in its operation. The DNS works a large, distributed, and structured database for resolving readable domain names into corresponding and valid Internet Protocol (IP) addresses [16]. The creation of DNS began in the 1980s, with the emergence of the Advanced Research Projects Agency Network (ARPANET) [14]. The DNS concepts and standards were published in Request for Comments (RFC) 882 and 883, updated later in RFCs 1034 and 1035. These standards are still relevant today and widely used [12].

Different DNS protocol approaches and implementations make it possible to offer users varying levels of performance and security. DNS is also used as an instrument for doing business, with various organizations offering domain resolution as

Institute of Informatics (INF) – Federal University of Rio Grande do Sul (UFRGS)
Porto Alegre, Brazil
E-mail: [marceloalmeida.silva, mffranco, ejscheid, lzembruzki, granville]@inf.ufrgs.br

a service (*i.e.*, DNS resolvers) focusing on providing better performance or security for users and services. Private DNS servers can offer services that guarantee security, privacy, and performance for users willing to pay for such services [9]. In addition, there is also the possibility of local DNS servers, which can be installed in the user's infrastructure (*i.e.*, companies) and provide more agility in name resolution. However, in both scenarios, there are trade-offs between costs, complexity of operation, and security [8].

Public DNS servers have emerged as an option to meet this demand efficiently, reliably, and at no cost. These servers are free and reliable DNS resolvers offered by large companies that maintain Internet services (*e.g.*, Google, Cloudflare, and Cisco). Public DNS servers can also provide security-related features, specifically for identifying malicious domains [1]. However, public DNS servers are a growing concern in academia and industry due to the centralization of services, network flows, and infrastructure [19]. In addition, outsourcing services to public DNS resolution companies that do not adopt adequate security measures can create risks for users of the service since name resolution can be negatively affected in cases of malicious attacks, such as Amplification, Spoofing, and Denial-of-Service (DoS) [7, 20].

In this context, the current literature focuses on approaches related to identifying and quantifying DNS centralization [3, 15]. However, most research does not analyze the performance of public DNS resolver servers in depth (*e.g.*, considering the popularity of domains and times of use), nor does it place the necessary emphasis on the steps to define approaches that measure such performance [6]. Therefore, there is an opportunity and the necessary motivation for approaches that analyze the performance of public DNS resolvers.

In this work, we propose PerfResolv, an approach to evaluate the performance of public DNS resolver servers in different locations worldwide using domain names with varying levels of popularity taken from various domain lists. To this end, the performance of the different Public DNS resolvers (*e.g.*, Google, Cloudflare, and Quad9) is collected and measured, and the measurements obtained are analyzed and compared according to different criteria, such as time of day, day of the week, and geolocation. The Tranco list [13] is used as the list of domains to be used and analyzed based on its popularity. The results provide an overview of the factors affecting their performance, including security, domain popularity, and geolocation as crucial factors.

The rest of this work is organized as follows. Section 2 examines the related work. Section 3 describes the PerfResolv approach, while Section 4 reports the results obtained using the PerfResolv and discusses the findings. Finally, Section 5 concludes the paper and presents opportunities for future work.

2 Related Work

The performance analysis of DNS resolvers is essential since users look for servers offering a better trade-off between security and performance. A literature review was conducted to understand the performance measurement scenario of DNS resolvers

and their different security levels over the last five years. Based on this, eight studies were selected and compared with the proposed PerfResolv. A summary of the analysis carried out is shown in Table 1.

The columns (*cf.* Table 1) represent the different attributes analyzed, including which DNS protocols were used and which metrics were collected for evaluation. The number of resolvers used and whether works considered domain popularity were also considered in the analysis performed. In addition, it was checked whether datasets with the results of the measurements are available, as well as whether the measurements were carried out in a geo-distributed manner (*i.e.*, different global collection points). Finally, the list of domains used as a basis for the work is listed when available.

Table 1: Comparison of Related Work on Analysis of DNS Performance

Work	Description	DNS Protocol	Metrics	Number of Resolvers	Popularity of Domains	Distributed Measurements	List of Domains
[4]	Centralized analysis of DoH and local DNS performance in a university network	Do53, DoT, DoH	DNS query time, Page load time	4	No	No	No
[10]	Analysis of the performance of DNS protocols and the impacts of encryption through Web page loading time	Do53, DoT, DoH	Page load time, DNS lookup time	3	No	Yes	Tranco 1M
[6]	Performance analysis of DNS servers using RIPE probes	Do53	DNS lookup time	10	No	Yes	Alexa Top 1M
[5]	Performance analysis of different DNS implementations on the BrightData network	DoH, Do53, DNSSEC	Page load time	4	No	Yes	No
[17]	Web tool that tests the performance of more than 200 global servers, supporting dozens of different public and private resolvers.	Do53	DNS lookup time	Variable	No	Yes	No
[1]	Analysis of the performance of local and public DNS servers in relation to malicious domains and their impacts on Web page loading time	Do53, DoH	DNS lookup time, Page load time	5	No	No	Cisco Top 1M Cisco umbrella
[11]	Analysis of the performance of DNS protocols in Web page loading time	DoT, DoH, Do53, DoTCP, DoQ	Page load time	313	No	Yes	Tranco 1M
[2]	Performance analysis of DNS servers violating TTL in the BrightData network	DNSSEC, DoH	DNS lookup time	27,000	No	Yes	Tranco 1M
This work (PerfResolv)	Analysis of the performance of public DNS resolvers concerning the popularity of domain names	Do53	DNS lookup time	5	Yes	Yes	Tranco 1M and new (unpopular) domains

Different studies have analyzed the performance of the traditional DNS (Do53), DNS over TLS (DoT), and DNS over HTTPS (DoH) protocols. [4] investigated the exploration of the political implications of DoH by measuring its performance compared with conventional DNS. In [10], the authors present measurements of how encryption using DNS Security Extensions (DNSSEC) affects the end-user experience in web browsers. In another paper, [6] checked the impact on reliability, security, and response time caused by DNS centralization.

The work [5] presented an approach to measuring DoH and Do53 performance called BrightData. In this work, the authors measured the protocols' performance on 22,052 customers at 224 collection points in different countries. Similarly, the DNSPerf tool [17] provides latency test results from more global collection points

every minute. During the tests, DNSPerf uses a variable number (from dozens to hundreds) of different public and private resolvers. Also focusing on performance, [1] analyzed the DNS resolvers used by an Italian Internet Service Provider (ISP) to compare them with the public resolvers provided by Google and Cisco.

In [11], the authors analyzed the performance of the DNS protocol over the Quick UDP Internet Connection (QUIC) protocol, which Google proposed as a protocol alternative for the transport layer. In this work, the authors compared the response times of DNS-over-Quic (DoQ) compared to Do53 (both UDP and TCP), DoT, and DoH for single queries and evaluated their impact on Web performance and performed on DNS resolvers around the world. Finally, [2] presented an approach that measures the performance of DNS resolvers that violate Time-to-Live (TTL) using an HTTPS proxy service at five different collection points.

Thus, based on the literature review, it is possible to identify several studies focusing on performance and security aspects related to the DNS protocol and associated services. However, none of the studies analyzed used domain popularity as a metric for evaluation. Therefore, the PerfResolv approach is proposed throughout this article to measure how domain popularity can impact the response time of different public DNS resolver servers.

3 PerfResolv Approach

PerfResolv is proposed as an approach to automate *(i)* the process of measuring the performance of public DNS resolver servers and *(ii)* the analysis of domains with different levels of popularity. The measurements and analyses are done in a geo-distributed manner using monitors managed by PerfResolv.

In this way, PerfResolv allows a refined analysis of public DNS resolution servers and their performance levels (*i.e.*, average response time) for domains with different levels of popularity, such as frequently accessed (more popular) and new domains (less popular). The days of the week and times of use can also be analyzed to understand the Internet usage profile and its impact on the performance of public DNS resolution servers. GMT (Greenwich Mean Time) is used to help analyze measurements from different countries with different time zones.

The approach proposed and implemented by PerfResolv is shown in Figure 1, including the flows and components required for all phases. These components work from monitoring and collection to analysis of the data obtained.

During the monitoring and collection phase, the list of domains is initially defined for analysis and processed by the *Data Processor*. This processing separates domains according to their popularity (*i.e.*, based on their position in rankings and number of accesses). The domains are then forwarded to the *Monitor Manager*, which controls and communicates with geo-distributed monitors in different regions of the world (*e.g.*, specific countries or cities). The monitors run periodic queries (*e.g.*, per hour or days) for all the defined domains. These parameters and configurations can be adjusted according to experiment requirements to encompass different needs that network operators or companies might have.

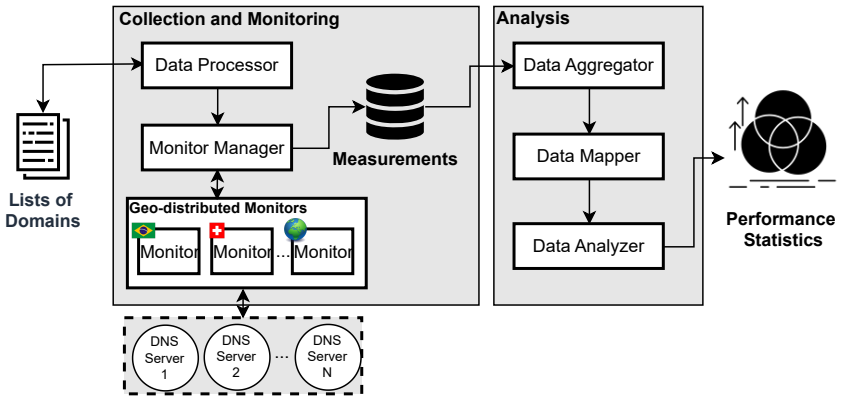


Fig. 1: PerfResolv's Architecture

For example, the monitors can be strategically distributed to observe the behavior of public DNS resolvers, which can vary in performance and security according to the domain, resolver, and region. During monitoring, measurements are taken for each domain for every query requested. All the measurements taken are forwarded to the *Monitor Manager*, which centralizes the measurements and stores them in a local database for later analysis.

During the analysis phase, the measurements are aggregated using the average of each domain's measurements per hour. Criteria for analysis are then defined and used to create subsets of the data, for example, filtered by country, DNS resolver, and domain type (popular and non-popular).

The implementation of PerfResolv and the data used is publicly available[1]. The PerfResolv monitoring and collection components were implemented using Python 3.11. The monitors use the *dnspython 2.3* library to resolve the domains in different public DNS resolvers and collect the performance measurements. The measurements are aggregated (*i.e.*, the average of the measurements taken for a domain at a given time) and mapped to Comma-Separated Values (CSV). The aggregated results are then analyzed using the *pandas 2.0.2* library. Finally, visualizations are generated using the *Vega-Altair 5.0.1* library.

4 Evaluation

The results obtained by applying the PerfResolv approach are discussed in this section. This allows us to understand the behavior of the different public DNS resolvers concerning domain popularity, time, and geolocation. The experiments were carried out by initially defining the IP addresses of the public DNS resolvers to be analyzed

[1] https://github.com/ComputerNetworks-UFRGS/PerfResolv

(*i.e.*, Google, Cloudflare, Comodo, OpenDNS, and Quad9), and the responses obtained were the response time to perform the query and receive the DNS response. These results can be accessed in the public PerfResolv repository and were processed to obtain aggregate statistics for analysis.

In total, 60 domains were selected, considering their popularity, for analysis: 20 of which were popular, 20 medium in popularity, and 20 completely new. Popular domains are extracted from the top of the Tranco list, where the medium are extracted from the position 300,000 (*i.e.*, still in the top 30% of the Tranco list). All the new domains were generated within a Brazilian academic and research network for this work only, thus ensuring they have little access or are permanently added to DNS caches worldwide. The experiments were conducted on Microsoft Azure Virtual Machines (VM) running in 3 countries (Australia, Brazil, and Switzerland), with 30 repetitions every hour for each domain and resolver. The period they covered was five days (Monday to Friday). In this way, it is possible to obtain the average of each execution cycle to improve the accuracy of our analysis.

Error bars were added for all plots in order to show the variability of the measurements collected. However, the bars are not prominent in the plots due to the slight error variance. Based on that, it is possible to conclude that the variance of the data is insignificant for our experiments.

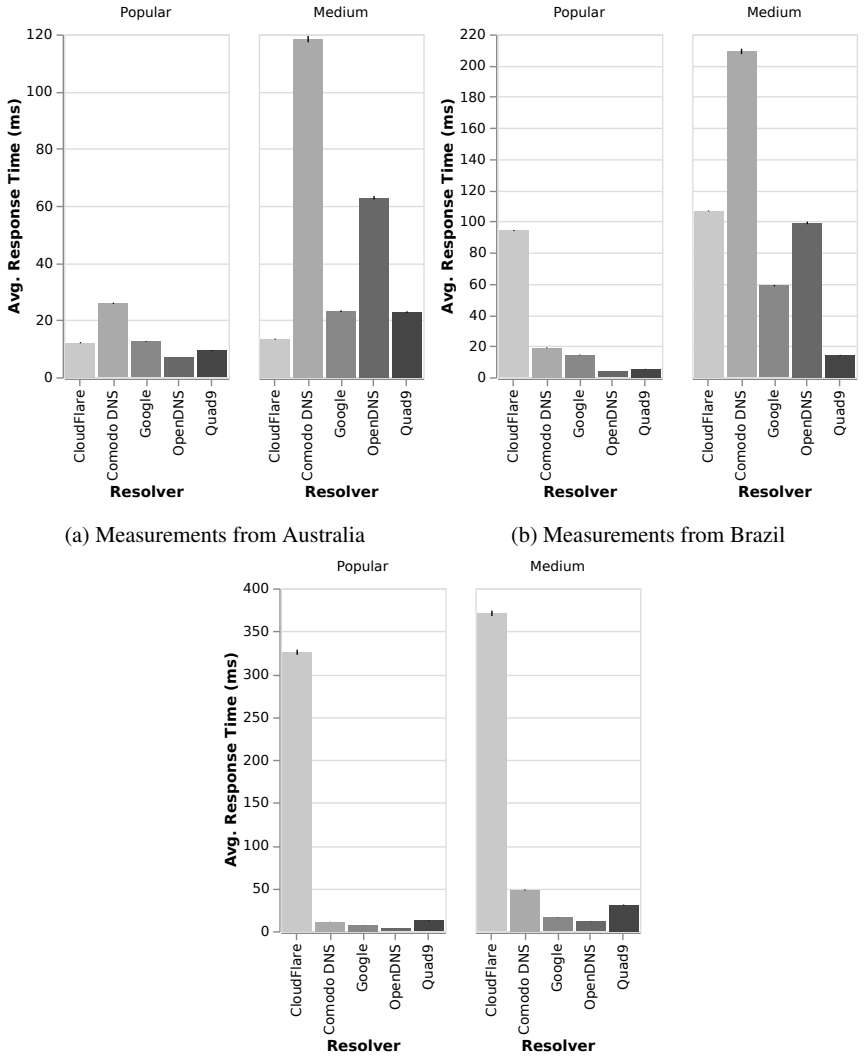
4.1 Popular Domains

The first analysis checks the response time for popular and medium domains. Thus, the performance of the resolvers in milliseconds (ms) is obtained for the resolution of domains with the most hits and known (*i.e.*, 20 most popular domains) and also for domains that are not so popular but are still known (*i.e.*, 20 domains with medium popularity). These domains were selected from the Tranco list.

The results are shown in Figures 2 (a), (b), and (c). Figure 2 (a) compares resolvers in Australia. The CloudFlare DNS resolver server performed best for popular and medium domains in this analysis. In contrast, the OpenDNS server performed worst for popular domains, and Comodo DNS performed worst for medium domains. On the other hand, the Google and Quad9 servers obtained similar performances for medium domains.

Figure 2 (b) compares the monitors in Brazil, where the Quad9 resolver have a better average performance in popular and medium domains, and Comodo DNS performed worse in medium domains. On the other hand, the Quad9 and OpenDNS resolvers have a similar performance in popular domains. However, when analyzing Cloudflare, it is possible to observe a discrepancy in performance for both popular and medium domains. As Cloudflare is known for having one of the best overall performances of public DNS resolvers, a more thorough analysis of which routing and security policies are implemented by the resolver specifically is necessary, as these policies can directly impact Cloudflare-related experiments.

Figure 2 (c) compares the resolvers through measurements taken by monitors located in Switzerland. The OpenDNS server performed best for popular and medium



(a) Measurements from Australia

(b) Measurements from Brazil

(c) Measurements from Switzerland

Fig. 2: Performance Analysis of Resolution Time for Popular and Medium Domains Observed from Different Countries

domains. Again, the CloudFlare server performed poorly on popular and medium domains. According to massive statistics from companies specializing in DNS monitoring and discussions with experts, an adequate domain resolution time should be no more than 100 ms and, in everyday situations, remain close to 20 ms [17].

In addition to domains with relevant popularity, new domains with few hits should also be analyzed to see how much the popularity impacts the resolution time. The results of the analysis of new domains are shown below.

4.2 New Domains

After analyzing popular domains, a list of new domains was also defined to check the impact of little-known and accessed domains on the resolution time of each server. For that, 20 *.br* domains were created in a Brazilian academic network, and the resolution time was compared with the other levels of popularity.

Figures 3, 4 and 5 show comparisons of resolver performance for popular, medium, and new domains for each of the countries used in the collection. The results show an impact on response times for new domains. For example, while the average response time for popular and medium domains was under 50 ms, the average for new domains was over 100 ms.

The measurements taken in Australia (*cf.* Figure 3) show that the performance of all resolvers was worse for new domains. This analysis indicates that OpenDNS performed much less well than the others for new domains and is the second worst for medium domains, even though it was a resolver that performed very well for popular domains.

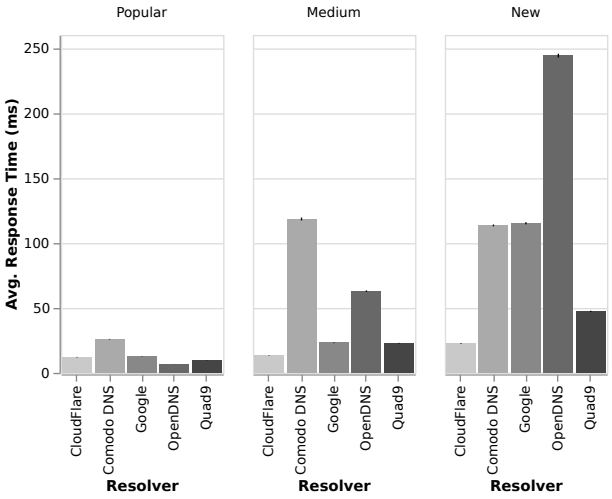


Fig. 3: Performance Analysis of New Brazilian's Domains Measured from Australia

In the measurements carried out in Brazil for new domains (*cf.* Figure 4), the Quad9 server obtained the best performance, while CloudFlare had the worst performance. It is important to note that all new domains have *.br* as their Country

Code Top Level Domain (ccTLD). Therefore, it is expected that all DNS resolvers would have the best performance for new domains for the Brazil data collection. However, this was not true for Cloudflare, which performed worse in Brazil than in Australia for such domains. Again, this may be because Cloudflare implements security policies that interfere with the experiments carried out.

In Figure 5, it can be seen that the OpenDNS server performed best for new domains when monitored from Switzerland, while Cloudflare performed worst for new domains.

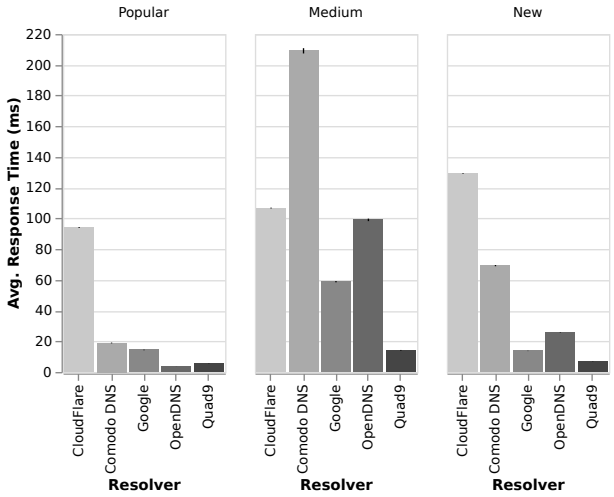


Fig. 4: Performance Analysis of New Brazilian Domains Measured from Brazil

Based on the results obtained, it is possible to gain insights into the differences in domain resolution according to their popularity and verify that some DNS providers handle requests differently, such as by implementing different security policies. The experiments conducted in Switzerland and Brazil were executed with varying implementations of DNS lookup tools (*e.g.*, dnspython and dig) [18] and using other machines in order to see if the reason for the behavior seen in the Cloudflare resolver could be related to implementation flaws or network limitations. However, the results showed no considerable variation. Therefore, it is important to carry out a thorough analysis not only of performance but also of other policies involving DNS resolution.

4.3 Discussion

The quantitative experiments show a considerable difference between the resolutions of popular vs. non-popular domains. This can be observed empirically and was proven valid - based on quantitative analysis - by following the PerfResolv approach. The geolocation of the measurement monitors (*i.e.*, where the requests are

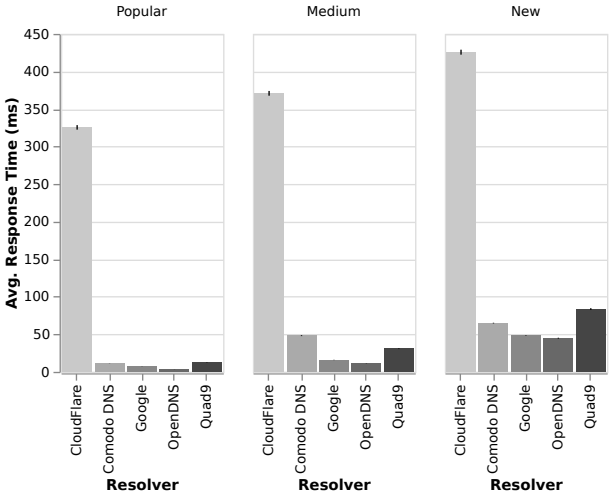


Fig. 5: Performance Analysis of New Brazilian's Domains Measured from Switzerland

made) directly impacts new domains that use ccTLDs from countries with unusual international access. For example, new *.br* domains have the worst performance compared to more popular domains when monitored from Switzerland and Australia.

In addition, it was possible to see that domains considered medium (in terms of popularity) can perform considerably poorly in some cases. This is because they are rarely accessed in specific locations. Therefore, domains that are popular on the Tranco list tend to be popular in all the locations analyzed (*e.g.*, facebook.com, google.com, and instagram.com). In contrast, medium domains (*e.g.*, shopiro.ca, freestart.hu, and tabsite.com) can be popular in specific locations and unpopular in others.

Furthermore, based on daily analysis, the days of the week did not impact the performance of DNS resolvers since all resolvers maintain a similar performance pattern from Monday to Friday. However, the time of day does generate some variations in performance. For example, the range from 10:00-12:00 and 14:00-16:00 hours have shown longer response times than others. The Cloudflare, Quad9, and Google resolvers remained stable but with some peaks during these periods. On the other hand, the OpenDNS and Comodo resolvers had much more constant fluctuations during the experiments, with response times varying by up to 40% between different times of the day.

5 Conclusions and Future Work

In summary, this paper presented the PerfResolv approach, a geo-distributed approach for analyzing the performance of public DNS resolvers based on the popularity of domains. The proposed approach allowed performance metrics to be collected, taking into account not only the performance of the resolvers but also the type and popularity of the domains. Using monitors located in three different countries (*i.e.*, Brazil, Switzerland, and Australia) and a list of 60 domains classified according to their popularity, experiments were conducted to evaluate the response time in resolving domain names with different levels of popularity (*i.e.*, popular, medium and new). The results made it possible to analyze how popularity affects the performance of DNS resolver servers.

The experiments indicated a considerable difference between the resolution time of popular and unpopular domains, impacted by the location of the measurement monitors. In addition, it was found that domains of medium popularity can perform poorly in some locations due to low access. Popular domains on the Tranco list are popular (*i.e.*, accessed frequently) in all the places analyzed, while medium domains are only popular in specific locations. Regarding the possible influence of the days of the week on the performance of DNS resolvers, there was no significant impact, thus maintaining a similar pattern from Monday to Friday. However, the time of day generated variations in performance, with mid-morning and mid-afternoon being the periods with the most extended response times. The oscillations identified in some DNS resolvers indicate a variation of up to 40% in response times over the different hours of the day.

Future work includes an analysis of the resolution time of unpopular domains in different resolvers, countries, and ccTLDs. This allows for a more comprehensive understanding of the impact of domain popularity on DNS resolver performance. In addition, it is important to investigate the trade-offs between security and performance to explore measures to improve resolver efficiency without compromising user security. Additional performance metrics, such as RTT and TTL, can be explored by PerfResolv to obtain a more complete and detailed view of DNS resolver performance. Finally, in-depth investigations of each DNS resolver analyzed should be conducted to mitigate the different oscillations and behaviors observed.

Acknowledgements This work was supported by The São Paulo Research Foundation (FAPESP) under the grant number 2020/05152-7, the PROFISSA project.

References

1. A. Affinito, A. Botta, G. Ventre: Local and Public DNS Resolvers: Do You Trade Off Performance Against Security? In: IFIP Networking Conference (Networking 2022). Catania, Italy, 2022, pp. 1–9
2. P. Bhowmick, M. I. Ashiq, C. Deccio, T. Chung: TTL Violation of DNS Resolvers in the Wild. In: International Conference on Passive and Active Network Measurement (PAM 2023). Berlin, Germany, 2023, pp. 550–563
3. D. F. Boeira, E. J. Scheid, M. F. Franco, L. Zembruzki, L. Z. Granville: Traffic Centralization and Digital Sovereignty: An Analysis Under the Lens of DNS Servers. In: 37th IEEE/IFIP

Network Operations and Management Symposium (NOMS 2024). Seoul, South Korea, 2024, pp. 1–9
4. K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, P. Schmitt: How DNS Over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem. In: 47th Research Conference on Communication, Information and Internet Policy (TPRC 47). Washington, D.C, USA, 2019, pp. 1–9
5. R. Chhabra, P. Murley, D. Kumar, M. Bailey, G. Wang: Measuring DNS-Over-HTTPS Performance Around the World. In: 21st ACM Internet Measurement Conference (IMC 2021). New York, USA, 2021, pp. 351–365
6. T. V. Doan, J. Fries, V. Bajpai: Evaluating Public DNS Services in the Wake of Increasing Centralization of DNS. In: IFIP Networking Conference (Networking 2021). Espoo and Helsinki, Finland, 2021, pp. 1–9
7. M. Franco, J. von der Assen, L. Boillat, C. Killer, B. Rodrigues, E. J. Scheid, L. Granville, B. Stiller: SecGrid: A Visual System for the Analysis and ML-Based Classification of Cyberattack Traffic. In: 46th IEEE Conference on Local Computer Networks (LCN 2021). Edmonton, Canada, 2021, pp. 1–8
8. S. Hao, H. Wang, A. Stavrou, E. Smirni: On the DNS Deployment of Modern Web Services. In: 31st IEEE International Conference on Network Protocols (ICNP 2015). San Francisco, USA, 2015, pp. 100–110
9. A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, N. Feamster: Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web. In: ACM/IRTF Applied Networking Research Workshop (ANRW 2019). Montreal Quebec, Canada, 2019, pp. 20–22
10. A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, N. Feamster: Comparing the Effects of DNS, DoT, and DoH on Web Performance. In: The Web Conference 2020 (WWW 2020). Taipei, Taiwan, 2020, pp. 562–572
11. M. Kosek, L. Schumann, R. Marx, T. V. Doan, V. Bajpai: DNS Privacy With Speed? Evaluating DNS Over QUIC and its Impact on Web Performance. In: 22nd ACM Internet Measurement Conference (IMC 2022). Nice, France, 2022, pp. 44–50
12. T. L. Lai, M. H. Tsai: Design and Implementation of a DNS Server With Geolocation Capability. In: 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS 2021). Tainan, Taiwan, 2021, pp. 370–373
13. V. Le Pochat, T. Van, S. Tajalizadehkhoob, M. Korczyński, W. Joosen: Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In: 26th Network and Distributed System Security Symposium (NDSS 2019). San Diego, USA, 2019, pp. 1–15
14. B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, S. Wolff: A Brief History of the Internet. Computer Communication Review **39**(5), 22–31, 2009
15. G. C. Moura, S. Castro, W. Hardaker, M. Wullink, C. Hesselman: Clouding Up the Internet: How Centralized is DNS Traffic Becoming? In: 20th ACM Internet Measurement Conference (IMC 2020). Pittsburgh ,USA, 2020, pp. 42–49
16. J. Park, A. Khormali, M. Mohaisen, A. Mohaisen: Where Are You Taking Me? Behavioral Analysis of Open DNS Resolvers. In: 49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2019). Portland, USA, 2019, pp. 493–504
17. PerfOps: DNSPerf - DNS Performance Analytics and Comparison, 2023, `https://www.dnsperf.com`
18. J. Pinto, E. Scheid, M. Franco, L. Granville: Analyzing and Comparing DNS Lookup Tools in Python. In: XX Escola Regional de Redes de Computadores (ERRC 2023). Porto Alegre, Brazil, 2023, pp. 49–54
19. L. Zembruzki, A. S. Jacobs, L. Z. Granville: On the Consolidation of the Internet Domain Name System. In: IEEE Global Communications Conference (GLOBECOM 2022). Rio de Janeiro, Brazil, 2022, pp. 2122–2127
20. L. Zembruzki, A. S. Jacobs, G. S. Landtreter, L. Z. Granville, G. C. Moura: Measuring Centralization of DNS Infrastructure in the Wild. In: 34th International Conference on Advanced Information Networking and Applications (AINA 2020). Caserta, Italy, 2020, pp. 871–882