International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 2 Article 4

January 2022

Experience a Faster and More Private Internet in Library and Information Centres with 1.1.1.1 DNS Resolver

Subhajit Panda
Chandigarh University, Mohali, Punjab, suvapanda007@gmail.com

Experience a Faster and More Private Internet in Library and Information Centres with 1.1.1.1 DNS Resolver

Cover Page Footnote

Acknowledgements: I would like to express my gratitude to our esteemed Professor Rupak Chakravarty (DLIS, Panjab University), who familiarised me with this concept and piqued my interest in conducting research in this field.

Experience a Faster and More Private Internet in Library and Information Centres with 1.1.1.1 DNS Resolver

1. Introduction:

Advances in information and communication devices during the past few decades have brought radical changes in the form of the information lifecycle. The Internet and the Web are constantly influencing the service model of library and information centres (LICs); their potential for delivering goods is quite vast, as they successfully overcome the geographical limitations associated with print media. LICs now use the Internet for efficient retrieval of information and meeting the dynamic information needs of the users.

According to Kemp (2021), in 2021, among the 1.39 billion population of India, 624.0 million used internet services in their daily life. Because of the large user base, India's ISP providers confront challenges in offering fast Internet services while maintaining a high level of security. To address these challenges, several LICs have begun to deploy a variety of DNS resolvers to deliver quick service to their users. While surfing the internet, for whatever purpose, we use DNS every time without knowing much about its functionality. DNS serves as a directory of names (domain names) that correspond to the numbers (IP address) (Shaw and Fruhlinger, 2020). In this study, The researchers focused on Cloudflare's 1.1.1.1 DNS resolver to examine if it is suitable for usage in LICs to deliver fast and secure internet services.

2. Domain Name System (DNS)

To access any resource on the Internet, a user must first find a server that hosts the requested resource. The IP address is the information locator on the World Wide Web, yet the human mind has trouble remembering such number strings. The Domain Name System (DNS) is the initial stage in this process, which converts a human-readable name (the resource hostname/ Domain name) into an IP address (Hours et al., 2015). DNS allows clients to use resolvers, sometimes called caches, to query a set of authoritative servers to translate host names into IP addresses (Shue and Kalafut, 2013).

2.1. DNS Resolver:

A DNS resolver, also called a recursive resolver, is a server setup of DNS, where the translation from domain name to IP address occurs (NS1, 2020) (Cloudflare, n.d.-b). In the process of resolving a DNS query, no interaction requires from the user's end apart from the initial request. There are 4 DNS servers involved in loading a webpage (Cloudflare, n.d.):

a) *DNS recursor* - The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers.

b) *Root nameserver* - The root server is the first step in translating (resolving) human readable host names into IP addresses.

c) *TLD nameserver* - This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname.

d) *Authoritative nameserver* - The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor that made the initial request.

These DNS servers accept the DNS queries from the user's end and response after solvinf through DNS resolver. In a typical DNS lookup three types of queries occur (Cloudflare, n.d.).

a) *Recursive query* - In a recursive query, a DNS client expects a DNS server (usually a DNS recursive resolver) to respond with either the requested resource record or an error message if the resolver is unable to locate it.

b) *Iterative query* - in this case, the DNS client will let the DNS server return the best possible result. If the requested DNS server cannot find a match for the query name, it will send the request to a DNS server that is authoritative for a lower level of the domain namespace. After then, the DNS client will query the referral address. This operation continues along the query chain with other DNS servers until an error or timeout occurs.

c) *Non-recursive query* - it will occur when a DNS resolver client asks a DNS server for a record that it has access to, either because it is authoritative for the record or because the record is in its cache. DNS records are typically cached by DNS servers to save unnecessary bandwidth usage and load on upstream servers.

3. Working Architecture between Browser and DNS Resolver

When a user types a URL address into their browser and presses Enter, the DNS Resolution process begins. The DNS must be resolved before the page and any resources on the page are loaded, so the browser can create a TCP connection to make the HTTP request. Furthermore, before the request is issued over HTTP, the DNS resolution must complete the identical procedures (per unique domain) for every external resource referred by a URL. The following steps presented a simplified working architecture between a browser and the DNS resolver (Catchpoint Systems, Inc., 2014).

3.1. *Step 1: OS Recursive Query to DNS Resolver* - When a user makes a query, the browser requests a specific page from the operating system, which then contacts a DNS resolver to answer the recursive query. The resolver must complete the recursion and return either an IP address or an error.

3.2. *Step 2: DNS Resolver Iterative Query to the Root Server* - The resolver starts by querying one of the root DNS servers for the IP of the query. If the query does not have the recursive flag and therefore is an iterative query associated with an address, the location of an authoritative name server, or an error.

3.3. *Step 3: Root Server Response* - The root server system consists of 13 root name servers and 1487 instances operated by the 12 independent root server operators over 380 different locations (root-servers.org, n.d.). These root servers hold the locations of all of the top-level domains (TLDs). The root does not have the IP information of the URL but it knows the server location. So it returns to the particular location of the server, listed in name server records.

3.4. *Step 4: DNS Resolver Iterative Query to the TLD Server* - The resolver then makes a query to one of the name servers connected with the requests to determine the location. Each TLD, like the Root Servers, has 4-13 clustered name servers spread over multiple locations. TLDs are divided into two categories: government-run country-code TLDs (ccTLDs) and generic TLDs (gTLDs).

3.5. *Step 5: TLD Server Response* - Each TLD server holds a list of all of the authoritative name servers for each domain in the TLD. As the gTLD server does not have the IP addresses for query url, it responds with a list of all of the NS records associated with the url.

3.6. *Step 6: DNS Resolver Iterative Query to the Name Server* - Finally, the DNS resolver queries one of name server for the IP of the query url.

3.7. *Step 7: NS Response from the query url* - This time the queried Name Server knows the IPs and responds with an A or AAAA address record (depending on the query type) for IPv4 and IPv6, respectively.

3.8. *Step 8: DNS Resolver Response to OS* - At this point the resolver has finished the recursion process and is able to respond to the end user's operating system with an IP address.

3.9. *Step 9: Browser Starts TCP Handshake* - At this point the operating system provides the IP to the application (browser), which initiates the TCP connection to start loading the page. For more information of this process, we wrote a blog post on the anatomy of HTTP.

4. 1.1.1.1 DNS Resolver

1.1.1.1 is a public DNS resolver operated by Cloudflare that offers a fast and private way to browse the Internet. Switching to a third-party DNS resolver has two key benefits: improved security and faster speed. 1.1.1.1 always uses strong encryption on their DNS or supports the DNSSEC security protocol, which protects DNS queries from data breaches and user devices from risks such as on-path attacks. The Cloudflare network, which spans over 250 cities worldwide, gives 1.1.1.1 a natural advantage in delivering fast DNS queries. Data centres in this network have access to the millions of Internet properties on the Cloudflare platform, ensuring users anywhere in the world get a lightning-fast response from 1.1.1.1 (query speed; 1.1.1.1 = 14.8ms, Cisco OpenDNS = 20.6ms, Google Public DNS = 34.73ms, Average ISP = 70.0ms) (Cloudflare, n.d.-a).

5. Set up 1.1.1.1 on User Device

Setting up 1.1.1.1 on any kinds of personal devices only required some steps to follow and no requirements of any technical skills or software proficiency.

5.1. Mobile Users:

For mobile users, iPhone and Android, Cloudflare launches 1.1.1.1 w/ WARP app available through Apple App Store (Apple Inc., 2022) and Google Play Store (Google, 2022), respectively. 1.1.1.1 with WARP replaces the connection between user's phone and the Internet with a modern, optimized, protocol. After install the apps, just one-touch setup and get a more private & faster Internet.

5.2. PC Users:

5.2.1. ***MacOS*** **-** Users with MacOS PC need to search for DNS Servers under System Preferences. After selecting it from the dropdown menu, add 1.1.1.1 and 1.0.0.1 DNS addresses (IPv4) in two successive DNS servers. For redundancy, users need to add two more DNS server with IPv6 DNS address: 2606:4700:4700::1111 and 2606:4700:4700::1001. Click Ok & Apply. The device is now ready with the 1.1.1.1 w/ WARP DNS resolver.

5.2.2. ***Windows*** **-** Windows PC required a change in adapter settings under 'Network and Internet' in 'Control Panel'. Under 'Change Adapter Settings', right-click the connected Wi-Fi network to select its 'Properties'. Now, as per requirements, users can change the properties of IPv4 from manual to 1.1.1.1 and 1.0.0.1 DNS addresses and for IPv6 from manual to 2606:4700:4700::1111 and 2606:4700:4700::1001 DNS addresses. Click Ok, Close & Restart the browser.

5.2.3. ***Linux*** **-** While these steps are for Ubuntu, most Linux distributions configure DNS settings through the Network Manager. Under Ubuntu based Linux system, at first click on the Application icon on the left menu bar, then select 'Settings' and then 'Network'. Find the connected network on the right pane, then click the gear icon. Under IPv4 or IPv6 tab change DNS settings from 'Automatic' (off) and enter manual DNS address 1.1.1.1 and 1.0.0.1 for IPv4 and 2606:4700:4700::1111 and 2606:4700:4700::1001 for IPv6.

5.3. Router: The router configuration may vary depending upon the manufacturer, model & connected network. In general, after connected to the preferred wireless network through router, in the router's configuration page, locate the DNS server settings. Replace existing DNS addresses to the 1.1.1.1 DNS address for IPv4 & IPv6.

6. Practical Implementation on Windows PC

In this study, the researcher tested the 1.1.1.1 DNS resolver with six different Windows PCs linked to ten distinct network connections with the same network providers. Before and after the setup (almost 1-10 minutes time interval), the upload and download speeds were tested one by one, and the enhanced speed percentage was determined to verify Cloudflare's standards.

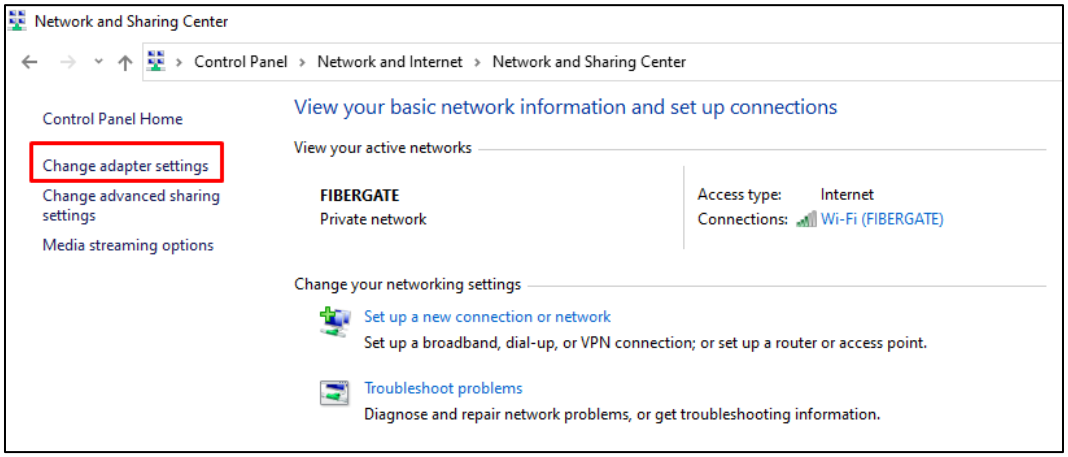
6.1. Implementation Steps:

For Windows PC, six simple steps required to follow for the configuration of 1.1.1.1 DNS resolver with preferred DNS addresses.

6.1.1. Step 1 **-** The configuration procedure begins with open-up the control panel of the PC. The Control panel can be accessed from the start menu or by typing its name into the 'search box' at the left corner of the PC.

6.1.2. Step 2 **-** To adjust connected network settings, under the Control panel "Network and Internet' option need to be selected and proceed further.

6.1.3. Step 3 **-**Under Network and Internet, click on "Network and Sharing Center" to view already connected network with the device.



(Control Panel > Network and Internet > Network and Sharing Center)

Figure 1: Changing the Adapter Settings

6.1.4. Step 4 **-**In this step the adapter settings of the already connected private network changed by selecting on "Change Adapter Settings" option. The six tested devices under this study connected with a private Wi-Fi connection (Fibergate from BSNL). *(see figure 1)*

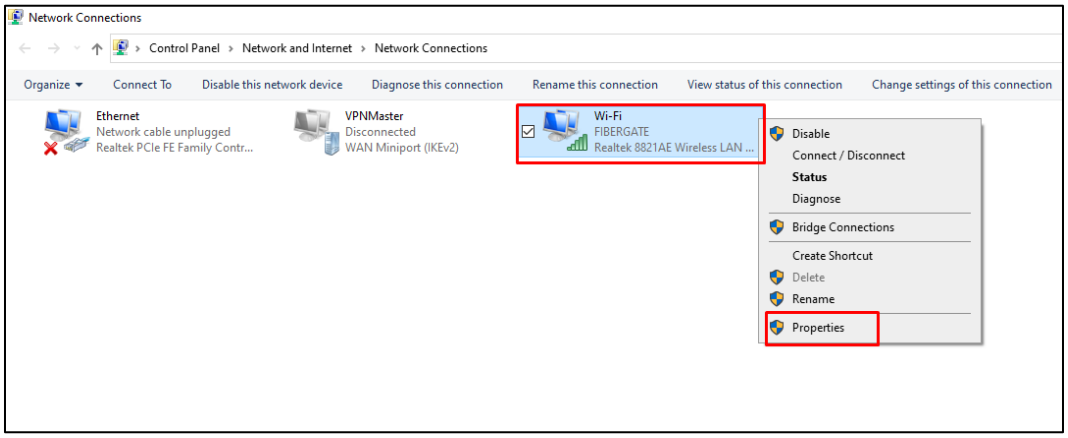


Figure 2: View the Properties of Already Connected Network

6.1.5. ***Step 5*** -Select the already connected Wi-Fi connection, right clickon it, then click on properties *(see figure 2)*.

6.1.6. ***Step 6*** -There are numerous network connecting elements under the "Networking" option of the Wi-Fi connection; pick Internet Protocol Version 4 (IPv4) or Version 6 (IPv6), as if required, then click on its properties again to update the DNS address *(see figure 3)*. The automated DNS server address must be set manually to alter the DNS address with IPv4 or IPv6 DNS addresses as mentioned below,

- For IPv4 DNS addresses: 1.1.1.1 and 1.0.0.1
- For IPv6 DNS addresses: 2606:4700:4700::1111 and 2606:4700:4700::1001

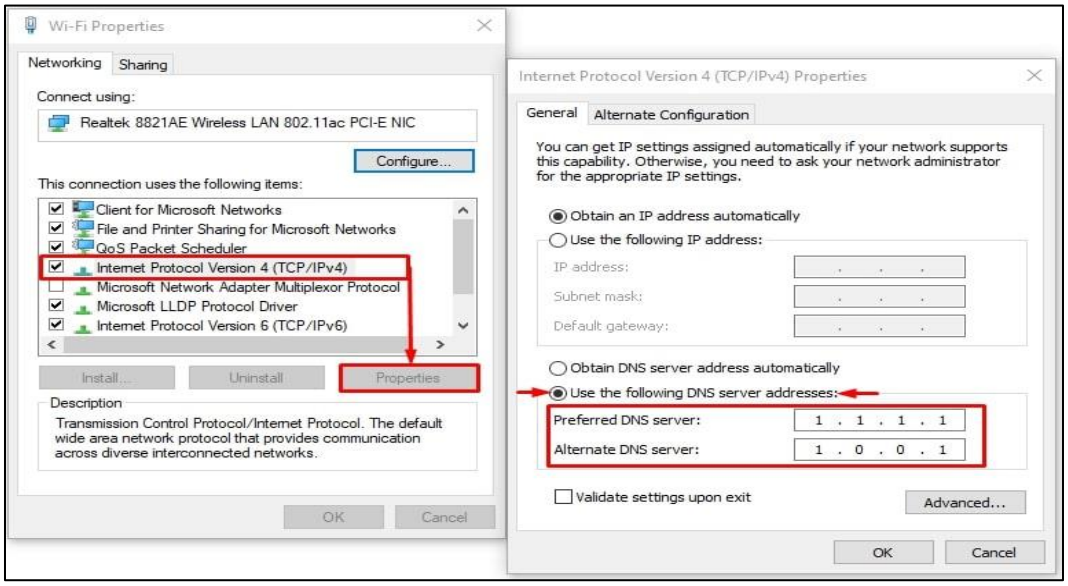


Figure 3: Configure Windows PC according to DNS 1.1.1.1 IPv4 Addresses

In this study the targeted six Windows PC connected with 1.1.1.1 IPv4 DNS connection. By altering IPv4 DNS addresses to 1.1.1.1 and 1.0.0.1, the six experimental Windows PCs (64 bits) were configured with the 1.1.1.1 DNS resolver *(see Figure 3)*. The ten network connection's ISP is BSNL Fibergate, and the internet connections' speed was measured using Measurement Lab and the nPerf online free internet speed checker in Chrome browser (v. 96.0) (Measurement Lab, 2022; nPerf, 2022). The internet speed were manually collected in a Microsoft Excel sheet *(see Table 1)* before and after the configuration and further analysed to evaluate the increase/decrease percentage.

Table 1: Internet Speed Measurement Table
(Before and After the Configuration of DNS 1.1.1.1 IPv4 Addresses)

SET I	PC 1				PC 2				PC 3			
	Before		After		Before		After		Before		After	
	D	U	D	U	D	U	D	U	D	U	D	U
NC 1	15.96	11.01	21.31	21.79	15.24	12.29	22.36	20.21	15.60	12.43	19.07	20.06

NC 2	15.71	10.51	21.05	22.72	15.26	11.98	22.65	19.90	15.42	11.94	20.03	21.17
NC 3	15.18	8.08	21.67	14.80	15.72	10.47	21.55	21.40	13.06	10.32	20.55	17.97
NC 4	14.36	9.14	20.68	17.27	15.97	10.40	19.68	20.20	13.26	8.30	20.28	20.63
NC 5	14.94	8.42	19.07	14.76	13.04	9.45	19.32	18.43	14.87	9.87	21.80	16.28
Total	76.15	47.16	103.78	91.34	75.23	54.59	105.56	100.14	72.21	52.86	101.73	96.11
Mean	15.23	9.43	20.76	18.27	15.05	10.92	21.11	20.03	14.44	10.57	20.35	19.22
Mean (SET I): D_{Before} = 14.91, U_{Before} = 10.31, D_{After} = 20.74, U_{After} = 19.17; Speed Increase (SET I): 39.10% (D), 85.94% (U)												
SET II	PC 4				PC 5				PC 6			
	Before		After		Before		After		Before		After	
	D	U	D	U	D	U	D	U	D	U	D	U
NC 6	16.28	12.23	23.18	21.18	17.26	14.11	21.42	20.85	16.08	13.76	21.48	20.74
NC 7	15.69	13.13	20.10	20.47	16.63	13.13	21.29	21.34	15.22	12.34	20.56	21.44
NC 8	15.76	11.45	23.01	19.13	18.90	14.45	23.14	21.02	16.53	11.69	20.19	21.83
NC 9	15.22	12.50	23.14	20.54	16.08	14.62	23.05	21.24	17.29	12.28	23.97	19.28
NC 10	16.14	10.05	20.43	21.22	17.14	15.07	22.70	24.77	16.90	11.40	22.85	20.42
Total	79.09	59.36	109.86	102.54	86.01	71.38	111.6	109.22	82.02	61.47	109.05	103.71
Mean	15.82	11.87	21.97	20.51	17.20	14.28	22.32	21.84	16.40	12.29	21.81	20.74
Mean (SET II): D_{Before} = 16.47, U_{Before} = 12.81, D_{After} = 22.03, U_{After} = 21.03; Speed Increase (SET II): 33.76% (D), 64.17% (U)												
Overall Mean: D_{Before} = 15.69, U_{Before} = 11.56, D_{After} = 21.39, U_{After} = 20.10; Overall Speed Increase: 36.33% (D), 73.88% (U)												

According to the study findings, the maximum download speed was identified as 18.90 Mbps among the six PCs before the setup to 1.1.1.1 DNS addresses, and the maximum upload speed was identified as 15.07 Mbps. The overall mean download speed was 15.69 Mbps, and the upload speed was 11.56 Mbps before the configuration. The highest download speed improved to 23.97 Mbps after the configuration was changed to the 1.1.1.1 DNS (IPv4) address, while it was 24.77 Mbps for upload. The aggregate mean download speed after configuration was 21.39 Mbps, and the upload speed was 20.10 Mbps. The study statistics indicated that, after configuring 1.1.1.1, internet speed improves by 36.33% for download and 73.88% for upload.

7. Benefits for the Library and Information Centers (LICs):

As technology has progressed, LICs have developed to meet diverse institutional and managerial demands. Libraries in the twenty-first century provide a welcome common space that invites students, teachers, and the broader community to explore, create, and collaborate. These bring together the best of print and electronic resources to develop learning hubs. To provide a meaningful contribution to this evaluation, 1.1.1.1 DNS resolver ensures a highly secured and

fastest internet services to cope with the current demand of the user-base. Here we can discuss some of such beneficial contributions of 1.1.1.1 to this aspect.

7.1. *Server load balancing* - 1.1.1.1 helps to balance the server load with a fast routing of connections between globally distributed data centers. It help LICs to find effective way to manage workloads and provide fastest ever services to their users.

7.2. *Internet traffic management* - 1.1.1.1 reducing network congestion and ensuring traffic flows to the appropriate resource in an optimal manner. 1.1.1.1 helps user to find the best possible answer for every DNS query by using Filters, a little programs that run inline for every DNS query.

7.3. *Multi-CDN* - If University level digital library services considered, a multi-CDN (Content Delivery Network) strategy can help in routing users that will reduce latency, improve performance, save costs and provide the best experience with lightning-fast services.

7.4. *Improve Secured Connection* - With increasing use of IOT devices in LICs also increase the risk of malware attacks in databases and servers. 1.1.1.1 always uses strong encryption on their DNS or supports the DNSSEC security protocol, which protects DNS queries from data breaches and user devices from risks such as on-path attacks.

7.5. *Geographical routing* - The primary objective of LICs is to provide users to their information need without any discrimination and in addition to it digital library services also eliminate the geographical boundaries. 1.1.1.1 help LICs in identifying the physical location of each user and ensuring they are outed to the nearest possible resource. It automate routing decisions based on the geography of the users and systems.

7.6. *Data center and cloud migration* - 1.1.1.1 ensures real-time integration of from on-premise resources to cloud resources in a controlled manner. Multi-cloud is a strategy for LICs seeking to prevent vendor lock-in, improve performance, reliability and reduce costs.

7.7. *Increase Connectivity* - 1.1.1.1 help LICs to connect app servers located in multiple locations, provide a fastest a single window interface for several databases and act as a middleware within a web application to reply DNS query. It also increase communication between IoT devices, and gateways.

The internet connections in India suffer from bandwidth pressure due to the enormous user base, resulting in a drop in speed and latency. The Indian education system has recently undergone a significant shift from physical to online learning. At the same time, to cope with it, LICs were under pressure to provide their services via the internet. However, to accomplish so, the entire work culture must be revised in accordance with contemporary user expectations. This online service and work culture of LICs encounters several challenges due to the low bandwidth of Internet connections in India. In this circumstance, using a safe and secure DNS resolver can assist in resolving the situation. Among these, the 1.1.1.1 DNS resolver, with its numerous benefits *(described 7.1-7.7 in this section)*, can assist LICs in obtaining a more private and faster network connection, allowing them to continue providing services without interruption.

8. Concluding Remarks:

Keeping aside the increasing demand and technological advancement, dealing with a natural calamity like the recent COVID-19 pandemic, LICs will turn to e-resources and digital library services as a last resort. The issue of network speed in a densely populated country like India is well-known, and citing the data from Computer Emergency Response Team (CERT-In), Cyberattacks amid the Covid-19 pandemic raised almost 300% last year (2020) to reach 1,158,208 compared to 394,499 in 2019 (Chauhan, 2021). The education sector in India has no exception from it. Due to the alarming rate of rising COVID-19 cases nationwide, the education system of India has taken a sharp turn towards e-learning, which causes a massive spike in Cyberattacks, mostly in the form of spear-phishing via Email, as one of the most preferred platforms. In such circumstances, one of the most critical demands of the LICs and education sectors is to find a safe and private network that also gives the quickest Internet speed. In this regard, Indian LICs commonly employ open DNS resolvers, although Cloudflare's 1.1.1.1 w/ WARP DNS resolver claims to be the most secure and quickest private network. This study supports the use of the 1.1.1.1 DNS resolver to boost Internet speed (36.33% for download and 73.88% for upload) and smooth surfing and also suggests that LICs may consider it after a comprehensive assessment on the institutional level.

References:

Apple Inc. (2022). *1.1.1.1: Faster Internet*. App Store. https://apps.apple.com/us/app/1-1-1-1-faster-internet/id1423538627

Catchpoint Systems, Inc. (2014, June 30). *DNS Lookup: How a Domain Name is Translated to an IP Address*. Www.catchpoint.com. https://www.catchpoint.com/blog/domain-name-to-ip-address

Chauhan, N. (2021, March 23). *Almost 300% rise in cyber attacks in India in 2020, govt tells Parliament*. Hindustan Times. https://bit.ly/2SCP68t

Cloudflare. (n.d.-a). *What is 1.1.1.1?* Retrieved January 12, 2022, from https://www.cloudflare.com/en-gb/learning/dns/what-is-1.1.1.1/

Cloudflare. (n.d.-b). *What Is DNS? | How DNS Works*. Retrieved January 12, 2022, from https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/

Google. (2022). *1.1.1.1: Faster & Safer Internet - Apps on Google Play*. Play.google.com. https://play.google.com/store/apps/details?id=com.cloudflare.onedotonedotonedotone

Hours, H., Biersack, E., Loiseau, P., Finamore, A., & Mellia, M. (2015, July 1). *A Study of the Impact of DNS Resolvers on Performance Using a Causal Approach*. LIG Laboratory - Grenoble Alpes University. https://lig-membres.imag.fr/loiseapa/pdfs/2015/Hours-etal_ImpactDNSCausal_ITC2015.pdf

Kemp, S. (2021, February 11). *Digital in India: All the Statistics You Need in 2021*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2021-india
Measurement Lab. (2022). *Measurement Lab Measure the Internet, save the data, and make it universally accessible and useful.* https://www.measurementlab.net/

nPerf. (2022). *Internet Speed test : Test your broadband connection - nPerf.com*. Www.nperf.com. https://www.nperf.com/en/

NS1. (2020). *What is DNS? DNS Explained*. https://ns1.com/resources/what-is-dns

root-servers.org. (n.d.). *Root Server Technical Operations Association*. Root-Servers.org. Retrieved January 12, 2022, from https://root-servers.org/

Shaw, K., & Fruhlinger, J. (2020, August 26). *What is DNS and how does it work?* Network World. https://www.networkworld.com/article/3268449/what-is-dns-and-how-does-it-work.html

Shue, C. A., & Kalafut, A. J. (2013). Resolvers Revealed: Characterizing DNS Resolvers and their Clients. *ACM Transactions on Internet Technology*, *12*(4), 1–17. https://doi.org/10.1145/2499926.2499928