INTERNATIONAL JOURNAL OF INFORMATIVE & FUTURISTIC RESEARCH (IJIFR)
ISSN: 2347-1697
VOLUME 13||ISSUE 5|| JANUARY 2026
An Open Access, Peer Reviewed , Globally Indexed & Refereed International Research Journal
Estd Year: 2013 || Website: www.ijifr.org || Email: editors@ijifr.org
Impact Factor=8.057, Index Corpenicus Value:6.62
Published By: Pioneering Journal Publishers

A COMPARATIVE STUDY OF ENCRYPTED DNS PROTOCOLS: DOT, DOH, ODOH, AND DOQ

Krishiv Taneja [1], Tiya Saluja [2]
[1,2] Student
B.Tech (Computer Science & Engineering)
Vellore Institute of Technology, Vellore, Tamilnadu, India

ABSTRACT:
The Domain Name System (DNS) is a key part of the Internet that translates human-readable domain names into numerical IP addresses. Most modern web traffic is now protected with encryption, but traditional DNS queries are still sent in plain text. This makes them vulnerable to threats like eavesdropping, manipulation, surveillance, and phishing attacks. This long-standing security issue has led to the creation of several encrypted DNS protocols aimed at improving privacy and data protection. The paper compares four main encrypted DNS protocols: DNS over TLS (DoT), DNS over HTTPS (DoH), DNS over QUIC (DoQ), and Oblivious DNS over HTTPS (ODoH). These protocols encrypt DNS queries in different ways and provide various levels of privacy, performance, and ease of use. DoT and DoH secure DNS traffic with TLS and HTTPS, respectively, which reduces the risk of interception and tampering. DoH has gained popularity because it integrates into well-known web browsers and operating systems. DoQ enhances performance by using the QUIC protocol, which reduces latency and avoids common transport issues, making it ideal for mobile and high-speed networks. ODoH improves user privacy by unlinking the client's identity from DNS queries, preventing any one entity from connecting users to their browsing habits. The paper also looks at the balance between privacy and performance, showing that stronger encryption can lead to extra latency, especially in unstable network conditions. It discusses how encrypted DNS affects Internet Service Providers (ISPs), network monitoring, and censorship. Adoption trends across different regions, platforms, and network types show steady growth, driven by default browser settings, mobile integration, and increasing awareness of privacy. Overall, the paper emphasizes that while no single encrypted DNS protocol works for every situation; each one plays a vital role in enhancing DNS security and privacy in today's Internet infrastructure.

KEYWORDS: ***DoT, DoH, ODoH, DoQ, DNS, Protocols, TLS***

PAPER CITATION:
Taneja,K, Saluja, T. : "A Comparative Study of Encrypted DNS Protocols: DoT, DoH, ODoH, and DoQ", International Journal of Informative & Futuristic Research (IJIFR), Vol.(13) (5), January 2026, pp. 609-615
DOI: https://doi.org/10.64672/IJIFR/26.01.13.5.033

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume 13(5), January2026

1. INTRODUCTION

The Domain Name System (DNS) is commonly referred to as the "phonebook of the Internet" converting names such as youtube.com or amazon.in into the machine-readable IP addresses 142.250.77.206. This hidden process occurs billions of times a day, yet actual DNS queries remain sent in plaintext over UDP port 53 (Do53), making them susceptible to eavesdropping, tampering, and redirection. Though the majority of web traffic uses HTTPS for protection, DNS has been slow to follow, leaving a vulnerable flaw that attackers use for eavesdropping, profiling, and phishing. Multiple encrypted DNS protocols have been standardized to redress these issues. DNS over TLS (DoT) encrypts queries with TLS via TCP port 853, while DNS over HTTPS (DoH) encapsulates them within HTTPS traffic to protect users from interception. DNS over QUIC (DoQ) offers encryption with improved performance using the QUIC protocol. Oblivious DoH (ODoH) adds an extra layer of privacy by preventing any one party from correlating a user's identity with their DNS queries. Combined, these protocols are a significant step towards safeguarding one of the Internet's most basic services. Encrypted DNS is significant in real-world usage as well as for network security. Firewalls and intrusion detection systems depend on DNS traffic to identify malicious activity, such as botnet communications and phishing attempts. Encrypted DNS also helps secure routine on- line activities, like viewing videos on YouTube, browsing Amazon, and messaging apps, by blocking tampering or profiling. Nonetheless, adoption remains skewed: user surveys on An- droid 9 Pie and Firefox indicate that the majority of users leave default DNS settings in place, frequently confusing their purpose or oblivious to alternatives. Complex interfaces and secret options constrain well-informed decisions as well, while encryption diminishes visibility to network operators, making it difficult for monitoring, detecting threats, and preserving network trust. This article further examines such developments through protocol differences, trends in deployment, performance trade-offs, resistance to censorship, and ISP conflicts, giving a well- rounded picture of the extant ecosystem for encrypted DNS.

2. BACKGROUND

The Domain Name System (DNS) is able to map human-friendly names to machine-understandable IP addresses, but its plain text architecture exposed it to interception and alteration. For better security and anonymity, newer protocols like DNS-over-HTTPS (DoH), DNS-over-TLS (DoT), Oblivious DNS-over-HTTPS (ODoH), and DNS-over-QUIC (DoQ) have emerged that are at varying levels of adoption and strength. DoH, standardized in RFC 8484, encrypts DNS traffic via HTTPS, mixing it with regular web traffic and making it difficult to block or identify. It has been broadly adopted by browsers such as Chrome, Firefox, and Edge, and proxy tools like Cloudflare's doh-proxy spread its use to system-level implementations. Although it defies hijacking and man-in-the-middle attacks, DoH has been argued about at times because it can evade network filters, creating debates on how to balance administrative control and privacy. Its ability to conceal itself in HTTPS traffic is a distinct feature that differentiates it from other protocols. DoT, by contrast, encrypts DNS queries across a reserved port (853) via a TLS handshake, where server and client authenticate one another and agree on secure keys. More tamper-resistant than plaintext DNS, its fixed-port dependency does make it simpler for censors or middleboxes to block it. Nevertheless, its handshake-based security is much stronger than more ancient methods. ODoH (Oblivious DNS-over-HTTPS) adds privacy by routing queries through a middle proxy, so neither party can correlate a user's identity with their request. This isolation intro- duces some delay and adds additional infrastructure, but it provides good privacy assurances, particularly when metadata leakage is an issue. DoQ (DNS-over-QUIC) provides DNS using the QUIC transport protocol, providing se- curity equivalent to DoT without the latency penalty and without the head-of-line blocking of TCP. Its lightweight, fast nature makes it a perfect fit for mobile networks and other latency- critical situations, though it has not yet been widely deployed. The combination of low-latency with robust transport-level security distinguishes it from other protocols. Together, they demonstrate the

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume 13(5), January2026

Internet community's attempts to make DNS more private and trustworthy. This critique examines their design trade-offs, performance effects, and de- ployment problems, providing an unambiguous vision of how encrypted DNS is building a secure Internet future.

Category	Criterion	DoH (DNS over HTTPS)	DoT (DNS over TLS)	ODoH (Oblivious DoH)	DoQ (DNS over QUIC)
Protocol Design	Application-layer protocol	Runs over HTTPS (port 443); blends with web traffic	Runs over TLS on TCP (port 853)	Same as DoH but adds proxy layer to decouple client IP and query	Runs over QUIC (port 784); reduces TCP inefficiencies
Security	Standard encryption	HTTPS (TLS) based; prevents eavesdropping	TLS-based encryption; strong but port-specific	DoH + end-to-end encryption between client & target; proxy blind	QUIC-based TLS 1.3 encryption; strong confidentiality
	Resistance to attacks	Prevents MITM, DNS hijacking; traffic blending can mask malicious flows	Prevents tampering/sniffing; failures due to blocking	Strongest privacy — proxy cannot link client and query	Prevents tampering; reduces latency-related attack vectors
Usability	Client-side impact	Integrated into Chrome, Firefox, Edge; transparent to users	Requires manual setup or OS support; failures 1.3–39% regionally	Extra latency due to proxy; requires support in resolvers	Lightweight for clients; efficient like UDP
	Latency	Higher than UDP due to HTTPS overhead	Lower than DoH but slower than UDP; TCP handshake adds delay	Higher than DoH (proxy adds hops)	Comparable to UDP; avoids TCP head-of-line blocking
Deployability	Protocol support	Widely deployed by browsers & proxies (Cloudflare, Mozilla, Google)	Supported by DNS software, but middleboxes drop port 853	Experimental; limited deployment, needs proxy infra	Draft-level; few real-world deployments so far
Maturity	Standardization	IETF standardized (RFC 8484)	IETF standardized (RFC 7858)	IETF draft (work in progress)	IETF draft (work in progress)
	Ecosystem support	Strong adoption; controversial for bypassing policies	Mature in some regions, unstable in others	Minimal adoption; active research area	Early stage; implementations scarce
Censorship Resistance	Ability to evade blocking	Strong — hard to block since it looks like normal HTTPS	Weak — easy to block (port 853 targeted by middleboxes/censors)	Strong — proxy separation hides client/query mapping	Moderate — uses port 784; less common, could be singled out
Compatibility	With existing systems	Very high — blends with HTTPS traffic, browser native	Medium — requires dedicated port & setup, blocked in some networks	Low-medium — needs proxy + target coordination	Medium — new transport (QUIC) not yet universally supported

Figure 1: Comparison of Encrypted DNS Protocols: DoT, DoH, ODoH, and DoQ

3. PRIVACY VS. PERFORMANCE TRADEOFF

Encrypted DNS queries are necessary to preclude surveillance, hijacking, and man-in-the- middle attacks, but privacy always carries a performance cost. Legacy DNS over UDP is quick
and light, but plaintext delivery leaves user queries vulnerable at several junctures of the res- olution process—between clients and resolvers, resolver logs, and in-transit nodes. Encrypted DNS protocols like DoT, DoH, DoQ, and ODoH try to close those privacy loopholes, but each adds new computational or communication overhead that impairs performance. Achieving a balance between protection of privacy and efficiency of performance has thus emerged as a key research challenge. DoT and DoH protocols depend on TLS and TCP, and involve extra round trips for hand- shakes and acknowledgments. These actions make confidentiality stronger but more expensive in terms of latency than plaintext DNS. Measurements in real-world situations reveal that un- der stable broadband conditions, the delay can be insignificant, but in unstable wireless or rural networks, the effect becomes perceptible—leading to slower query resolution times and even adoption minimization. Interestingly,

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume 13(5), January2026

performance is network type-dependent: in 3G networks, plaintext DNS performed better than both DoT and DoH, whereas in lossy 4G networks, DoT performed more robustly due to TCP's smaller timeout limits.

DoQ, on the other hand, is built on top of QUIC over UDP and adds optimizations like zero-RTT connection establishment. This minimizes head-of-line blocking and removes a lot of the latency overhead present in DoT and DoH, which makes DoQ all the more appealing in high-demand scenarios such as mobile networks. DoQ, however, remains in draft state, and its deployment is limited in comparison to the ubiquitous presence of DoH within browsers and operating systems. Privacy-oriented protocols such as ODoH take this concept one step further by detach- ing user identity from searches via an intermediary proxy. While this provides much bet- ter anonymity—preventing anyone from correlating a client's IP address with their DNS re- quests—it introduces additional hops, adding latency. The trade-off is evident: increased pri- vacy at the price of slower responsiveness. Likewise, protection mechanisms such as QNAME minimization cut down exposure of data by sending only pertinent parts of a query up the DNS tree, yet with each level of protection added, there is additional processing time. Aside from protocol mechanics, more fundamental structural problems make the balance between privacy and performance problematic. Most encrypted DNS resolvers are funneled through a handful of large service providers, potentially creating monopolies on data even if the transmission is encrypted. For performance, however these services frequently bundle resolvers with content delivery networks (CDNs), reducing latency for hosted content while incidentally favoring some services over others—reviving discussions on net neutrality. Ultimately, encrypted DNS protocols reflect the ever-present tension between performance and privacy. While DoT and DoH present better guarantees with the penalty of latency, DoQ gives near-UDP performance with encryption, and ODoH adds privacy at the expense of slow- ing resolution by proxying. The challenge to future study is crafting protocols and models of deployment that strike an equitable balance: maintaining user privacy without sacrificing DNS resolution to the point where it does not get pervasive adoption.

4. ISP CONFLICT AND CENSORSHIP

Internet censorship is the intentional restriction or control of online material by governments, regulatory bodies, or other institutions. It usually entails blocking websites, traffic filtering, or DNS response manipulation for the purpose of upholding legal, political, or cultural norms. Au- thoritarian governments, like China, exercise wide-ranging censorship through methods such as DNS injection, keyword filtering, and mass content blocking, notoriously achieved by way of the Great Firewall. Such policies limit access to information, seriously challenging free expression and online privacy. The advent of encrypted DNS protocols such as DNS-over-HTTPS (DoH), DNS-over-TLS (DoT), DNS-over-QUIC (DoQ), and Oblivious DNS-over-HTTPS (ODoH) provides partial cir- cumvention of these prohibitions. By encrypting DNS queries, these protocols hide traffic from intermediaries such as ISPs, making it unproblematic to manipulate or inspect. DoH and DoT enhance privacy by encrypting queries over HTTPS and TLS respectively, and DoQ optimizes performance with multiplexed, secure queries over QUIC. ODoH also enhances anonymity by separating the client's IP address from the DNS request, lowering the threat of profiling or surveillance. These technologies enable users, journalists, and activists to gain unfettered ac- cess to information, while also being used in businesses to provide secure and tamper-evident DNS resolution. Encrypted DNS, though, brings with it clashes with Internet Service Providers (ISPs) and regulation. ISPs have traditionally depended on DNS visibility to implement parental controls, content filtering, malware defenses, and legal requirements. Encryption restricts their ability to inspect traffic, bringing operational and legal burdens. Centralization of DNS resolution using big players like Google or Cloudflare further diverts traffic off domestic ISPs, with implications regarding surveillance, privacy, and anti-competitive behavior. Governments in some areas, like the UK and the U.S., that have laws requiring content monitoring or blocking might view

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume 13(5), January2026

encrypted DNS as subverting lawful supervision. This tension reveals a complicated balance: encrypted DNS enhances user privacy and cen- sorship circumvention but also makes ISP obligations and compliance more complicated. In the future, hybrid strategies—such as policy-conforming encrypted DNS resolvers, filtering by user consent, or selective monitoring—will perhaps be necessary to balance privacy, security, and governance. Generally, the competition between technological advancement, censorship circumvention, and ISP obligations reflects the complex challenges of governing the contem- porary Internet.

5. ADOPTION TRENDS IN ENCRYPTED DNS

The adoption of encrypted DNS has grown steadily over the last decade, reflecting rising aware- ness about online privacy, increasing cyber-attacks, and the spread of secure Internet standards. Protocols such as DNS-over-HTTPS (DoH), DNS-over-TLS (DoT), and DNS-over-QUIC (DoQ) — along with newer privacy tools like Oblivious DoH (ODoH) and Encrypted Client Hello (ECH) — are gradually replacing traditional unencrypted DNS. This shift is driven by the need to protect user browsing information from ISPs, intermediaries, and attackers, while also improving trust in network communication.

(i) **Global Adoption Pattern** Encrypted DNS usage is growing worldwide, although adop- tion levels differ by region, network type, and provider. Studies show that encrypted DNS initially formed a small portion of global DNS traffic, but it has steadily increased as browsers and operating systems began enabling it by default. Early measurements placed encrypted DNS usage around 13–14% of global DNS traffic, with recent industry estimates suggesting a rise toward 20–25% in some markets. Market research values the encrypted DNS services segment at approximately USD 1.42 billion in 2024, with projections reaching around USD 7.26 billion by 2033 — showing an expected CAGR of nearly 19%. This growth reflects increasing reliance on secure DNS in corporate environments, cloud services, and modern consumer devices.

(ii) Regional adoption trends include:

- Leads in deployment, supported by browser and OS defaults and the widespread use of public resolvers like Google and Cloudflare, accounting for about 38% of global en- crypted DNS usage.
- Europe: Enterprise adoption is growing, driven by privacy laws such as GDPR, with nearly 40% of organizations implementing DoH/DoT for internal or hybrid networks.
- Asia-Pacific: The fastest-growing region, projected to expand at ˜25%, fueled by digital transformation, mobile-first usage, and cloud adoption.
- Africa and Latin America: While overall adoption is lower, local successes are notable - APNIC reports around 12% DoH and 8% DoT usage, with some ISPs (e.g., in Senegal) achieving nearly 95% encrypted DNS traffic.

(iii) **Adoption by Platforms and Users:** Adoption is closely linked to platform support:

- Android 9+ includes *Private DNS* using DoT.
- Windows 10/11, iOS, macOS, and Linux support encrypted DNS configuration.
- Browsers such as Chrome, Firefox, Opera, and Edge offer multiple DoH modes (Off / Opportunistic / Strict).

A user survey found:

- 67% selected Opportunistic mode,
- 20% chose Strict mode,
- 13% disabled encryption.

These results highlight how defaults drive adoption. For instance, when Firefox enabled DoH by default in the U.S. (2020), encrypted DNS usage surged significantly. Industry re- ports estimate that over one billion devices now ship with encrypted DNS enabled or easily configurable.

(iv) **Differences Across Networks and Sectors:** Adoption also varies by context:

- Consumer networks: Rapid growth due to browser defaults and mobile integration.

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume 13(5), January2026

- Enterprises: Gradual adoption as part of Zero-Trust and cloud security frameworks (39– 43% partial adoption by 2024).
- Cloud and CDN providers: Google, Cloudflare, and Quad9 handle billions of encrypted DNS queries daily.
- Mobile networks: Increasingly testing DoQ for improved latency and connection perfor- mance, particularly in 4G/5G environments.

(v) **Performance and Availability Insights** Performance concerns, once a major barrier, have reduced considerably:

- Encrypted and plaintext DNS perform comparably on stable connections.
- In wireless setups, DoT can outperform DoH, while DoQ shows even lower latency due to faster connection setup.
- Studies report that over 99% of global clients can now reach encrypted resolvers, showing strong infrastructure readiness.

(vi) **Challenges Affecting Adoption** Despite significant progress, challenges remain includ- ing lack of user awareness, centralized resolver dependence, and administrative resistance from ISPs. Yet, with continued platform support and user education, adoption is expected to expand steadily in the coming years.

Challenge	Description
Centralization	Reliance on a few global providers (Google, Cloudflare) raises privacy and trust concerns
ISP opposition	Some ISPs express concerns about loss of filtering and parental-control capabilities
Enterprise visibility	Encrypted DNS limits monitoring for threat detection unless special tools are used
Complex configuration	Resolver discovery standards are still evolving, slowing automatic deployment
Policy differences	Countries with strict control over DNS may block encrypted protocols

Figure 2: Challenges in Adoption of Encrypted DNS Protocols

6. FUTURE DIRECTIONS

Beyond the widely adopted DoT, DoH, ODoH, and DoQ, several other encryption approaches have been proposed to strengthen DNS privacy. **D**NS-over-DTLS functions similarly to DoT but operates over UDP instead of TCP, providing faster handshakes and reduced latency. How- ever, due to limited support and deployment, it remains largely experimental and is typically considered a backup option for DoT in scenarios demanding lower connection overhead. **D**NSCrypt, introduced in 2011, predates many modern encrypted DNS protocols. It em- ploys the *X25519-XSalsa20Poly1305* cryptographic suite rather than TLS, offering robust en- cryption while transmitting over port 443 — blending effectively with regular HTTPS traf- fic. Despite lacking IETF standardization, DNSCrypt has seen adoption by resolvers such as *OpenDNS*, *OpenNIC*, and *Yandex*. It requires clients to install the DNSCrypt-proxy application and resolvers to manage certificate signing using specialized hardware, which has somewhat limited mainstream deployment. Finally, DNSSEC (Domain Name System Security Extensions) ensures the authenticity and integrity of DNS data by digitally signing responses. While DNSSEC does not encrypt traffic, it complements DNS-over-encryption methods like DoT or DoH, offering layered protection where one ensures integrity and the other ensures confidentiality. Ongoing research continues to explore optimizing DoH scalability in high-traffic networks and improving

mechanisms that balance privacy with necessary network monitoring and filtering capabilities.

7. CONCLUSION

Each encrypted DNS protocol offers distinct advantages tailored to specific use cases. **D**NS- over-HTTPS (DoH) is ideal for everyday users, as its integration into browsers enhances acces- sibility and enables circumvention of network censorship. DNS-over-TLS (DoT), on the other hand, provides standardized security suited for enterprise or managed networks, though its use of a dedicated port makes it more vulnerable to blocking. Oblivious DNS-over-HTTPS (ODoH) takes privacy a step further by separating client identity from DNS queries, but faces challenges related to added latency and limited real-world deployment. **D**NS-over-QUIC (DoQ) emerges as a promising candidate for latency-sensitive environments such as mobile networks, leverag- ing QUIC's faster handshake and reduced connection overhead. Looking ahead, research continues to refine these protocols toward better scalability, re-duced performance trade-offs, and broader interoperability. Efforts are also underway to merge privacy-oriented mechanisms like ODoH with high-speed transports like DoQ, potentially of- fering the best of both privacy and efficiency. As encrypted DNS becomes more pervasive, striking the right balance between privacy, performance, and policy compliance will remain central to the evolution of secure Internet infrastructure.

8. REFERENCES

[1] M. Dawood, S. Tu, C. Xiao, M. Haris, H. Alasmary, M. Waqas, and S. U. Rehman, "Dns over https: An overview of privacy and performance improvements," *Journal of Network and Computer Applications*, 2024.

[2] A. Gupta, R. Sharma, and K. Verma, "An insight into encrypted dns protocol: Dns over tls," in *2021 6th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, 2021.

[3] W. Li, J. Zhang, and M. Chen, "A survey on dns encryption: Current development, malware misuse, and inference techniques," *ACM Computing Surveys*, 2022.

[4] R. Kumar and A. Singh, "Dns encryption and censorship-resistant communication: A modern analysis," *arXiv preprint arXiv:2312.04577*, 2023.

[5] T. Zhou *et al.*, "A privacy analysis of dns-over-encryption protocols," in *Network and Distributed System Security Symposium (NDSS DNS Privacy Workshop)*, 2021.

[6] M. NADAF, "Dns over https: User awareness and implementation challenges," *Interna- tional Journal of Creative Research Thoughts (IJCRT)*, 2023, paper ID: IJCRT23A6012.

[7] S. Singanamalla, K. Fawaz, and P. Schmitt, "Oblivious dns-over-https (odoh): Practical privacy for dns queries," *Proceedings of the ACM on Computer Communication Review*, 2021.

[8] K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, and P. Schmit, "How dns over https is reshaping privacy, performance, and policy in the internet ecosystem," *Communications of the ACM*, 2021.

[9] Z. Lu *et al.*, "A large-scale measurement study on the adoption of encrypted dns," *arXiv preprint arXiv:2107.04436*, 2021.