Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.050049

REVIEW

The Impact of Domain Name Server (DNS) over Hypertext Transfer Protocol Secure (HTTPS) on Cyber Security: Limitations, Challenges, and Detection Techniques

Muhammad Dawood[1], Shanshan Tu[1], Chuangbai Xiao[1], Muhammad Haris[2], Hisham Alasmary[3], Muhammad Waqas[4,5,*] and Sadaqat Ur Rehman[6]

[1]Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China

[2]National Center of Robotics and Automation, University of Engineering and Technology, Peshawar, 25000, Pakistan

[3]Department of Computer Science, College of Computer Science, King Khalid University, Abha, 61421, Saudi Arabia

[4]School of Computing and Engineering Sciences, Faculty of Engineering and Science, University of Greenwich, London, SE10 9LS, United Kingdom

[5]School of Engineering, Edith Cowan University, Perth, WA 6027, Australia

[6]School of Computer Science and Engineering, University of Salford, Manchester, M54BR, United Kingdom

*Corresponding Author: Muhammad Waqas. Email: engr.waqas2079@gmail.com

Received: 26 January 2024 Accepted: 07 August 2024 Published: 12 September 2024

ABSTRACT

The DNS over HTTPS (Hypertext Transfer Protocol Secure) (DoH) is a new technology that encrypts DNS traffic, enhancing the privacy and security of end-users. However, the adoption of DoH is still facing several research challenges, such as ensuring security, compatibility, standardization, performance, privacy, and increasing user awareness. DoH significantly impacts network security, including better end-user privacy and security, challenges for network security professionals, increasing usage of encrypted malware communication, and difficulty adapting DNS-based security measures. Therefore, it is important to understand the impact of DoH on network security and develop new privacy-preserving techniques to allow the analysis of DoH traffic without compromising user privacy. This paper provides an in-depth analysis of the effects of DoH on cybersecurity. We discuss various techniques for detecting DoH tunneling and identify essential research challenges that need to be addressed in future security studies. Overall, this paper highlights the need for continued research and development to ensure the effectiveness of DoH as a tool for improving privacy and security.

KEYWORDS

DNS; DNS over HTTPS; cybersecurity; machine learning

1 Introduction

Domain Name System (DNS) traffic is critical in modern security systems. Translating domain names into Internet Protocol (IP) addresses through DNS is necessary for establishing connections, and it can also reveal potential security risks in network traffic. Security systems can use this

Copyright © 2024 The Authors. Published by Tech Science Press.
This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

information using the readable translated domain names in the traffic. Application firewalls use this information to enforce security policies and intrusion detection systems to identify suspicious connections, such as botnet activity. DNS over HTTPS (DoH) is a way to secure the communication between a user's device and a DNS resolver. Traditional DNS communication is done through plain-text queries, which can be easily intercepted and compromised. To address this security concern, DoH encrypts the DNS queries and sends them through a Hypertext Transfer Protocol Secure (HTTPS) connection, making the communication more secure and protecting the user's information from being exposed. The increased privacy helped prevent user profiling and targeted advertising. Despite only being published in 2018, DoH has already become widely adopted as a solution to the privacy concerns of traditional DNS.

Secure Socket Layer/Transport Layer Security (SSL/TLS) protocol is the standard encryption method used for secure communication between client and server over the web using HTTPS. This helps to protect the content of their communication from being seen by third parties. When accessing an HTTPS web server, the client must first find the server's domain name, usually done through a plain text DNS request. DNS over HTTPS (DoH) is a new approach where DNS queries are included within the secure HTTPS protocol.

This encryption provides several key benefits:

I. By encrypting the entire query and response, third-party observers cannot see the contents of the communication. This protects user privacy by preventing the collection of information about the websites they visit. On the other side, encrypting the DNS traffic also protects against tampering with the query or response by attackers. This makes it harder for attackers to redirect users to phishing sites or interfere with their access to legitimate websites.

II. Using SSL/TLS [1] encryption, DoH enhances the privacy and security of the Internet's DNS and provides a more secure method for performing DNS lookups. The latest versions of popular web browsers, such as Firefox and Google Chrome, have integrated support for DoH. This means that users can use DoH directly from within these browsers. However, if a user runs an older web browser version that lacks DoH support or prefers an alternative method, they can install proxy software like Cloudflare, doh-proxy, dnscrypt-proxy, or doh-client. This software can encrypt all domain name resolution requests made from the client system, providing enhanced privacy and security. By using DoH with proxy software, users can guarantee that all of their DNS requests are encrypted and secure, regardless of the underlying operating system or web browser's lack of built-in DoH support issues [2].

In the past, cybercriminals used DNS to communicate with each other secretly. This type of communication, a covert channel, is used to hide the transmission of information from being detected. By exploiting the DNS protocol, attackers can evade security measures and carry out malicious activities, making it difficult for network administrators to identify and prevent such activities. The encryption feature of DoH complicates the situation by making it impossible to analyze the traffic, including the domain names being queried and the related metadata [3]. Over the past few years, several techniques for encrypting DNS communication have been devised, tested, and implemented to safeguard user security and privacy. They were first launched in 2008 and 2011 and include DNSCurve and DNSCrypt [4] respectively and aimed to encrypt DNS traffic between clients and servers to prevent outsiders from intercepting or modifying it [5].

However, these early proposals were not widely adopted, as they were not standardized, which meant that different implementations could cause interoperability issues between clients and servers. To address this issue, the Internet Engineering Task Force (IETF) proposed a series of standards

Request for Comments (RFCs), which started in 2016, to promote the adoption of DNS encryption. These standards, like DNS over QUIC, DNS over TLS (DoT), and DNS over HTTPS (DoH). User Datagram Protocol Internet Connections (DoQ) rely on existing secure protocols to encrypt DNS traffic. DNS over TLS (DoT) [6] uses the Transport Layer Security (TLS) protocol to encrypt DNS queries and responses, providing end-to-end encryption between clients and servers. DoT is compatible with existing DNS infrastructure and can encrypt DNS traffic without modifying the existing DNS protocol. DoH is a technology that improves the privacy of internet users by encrypting their DNS queries [7].

The encryption of DNS traffic differs between traditional DNS and DNS over HTTPS (DoH). Traditional DNS transmits queries and responses in plaintext, allowing security devices easy inspection and analysis. In contrast, DoH encrypts DNS traffic within the HTTPS protocol, securing communication between the client and the DNS resolver. While this encryption enhances privacy and prevents eavesdropping, it poses a challenge for security devices, as they lose direct visibility into the content of DNS queries. This shift prompts a trade-off between strengthened privacy and the ability of security systems to inspect DNS traffic effectively. The transition to DNS over HTTPS (DoH) results in a loss of visibility for network security devices. In traditional visibility, security devices depend on clear-text DNS traffic to scrutinize domain names, recognize patterns, and identify potential threats. However, the encryption introduced by DoH means that security devices no longer have access to the details of DNS queries in plaintext. Instead, they encounter only encrypted data, posing a challenge to their ability to effectively analyze and identify potential threats. This shift highlights a trade-off between enhanced privacy through encryption and the diminished visibility for security systems in monitoring DNS activities. The increased attack surface resulting from the encryption of DNS queries, especially in the context of DNS over TLS (DoT), poses notable challenges to traditional security systems. In traditional DNS setups, queries and responses are typically transmitted in plaintext, allowing security devices to inspect and analyze them for potential threats. However, the landscape changes with the adoption of encryption in DNS, as seen in DoT.

DoT secures DNS traffic by encrypting it during transmission, enhancing privacy but complicating the ability of traditional security systems to inspect the content of DNS queries. The encryption of DNS queries hinders the visibility of network security devices, as they can no longer easily analyze the plaintext DNS traffic for malicious activities. This change, like DNS traffic, from clear-text to encrypted, results in an expanded attack surface.

However, despite the benefits of privacy, DoH still has some security vulnerabilities, as it is built on the same underlying principles as the traditional DNS, which has its own set of security. This paper presents a comprehensive review of the impact of DoH on cyber security. We discuss the limitations and difficulties associated with the implementation of DoH. Furthermore, we will discuss DoH abuse on the internet and various techniques for detecting DoH tunneling. Finally, we identified several critical research challenges that can be focused on in future security studies, as shown in Fig. 1.

This paper's contributions can be summed up as follows:

I. We provide a comprehensive review of the impact of DoH on cyber security, including limitations, implementation difficulties, and instances of abuse on the internet.
II. We discuss various techniques for detecting DoH tunneling and identify key research challenges for future security studies.
III. We raise awareness of the potential security issues associated with DoH and promote a better understanding of the risks and challenges associated with this technology to facilitate the development of effective security solutions to address them.

IV. We highlight the importance of prioritizing security measures while implementing DoH, which is crucial for ensuring user privacy and data protection.

V. We outline significant research challenges and areas for future study related to DoH, including compatibility with existing DNS infrastructure, standardization, privacy, user awareness, impact on network security, blocking or filtering, and ensuring DoH security.

Fig. 1 highlights the roadmap for this study.

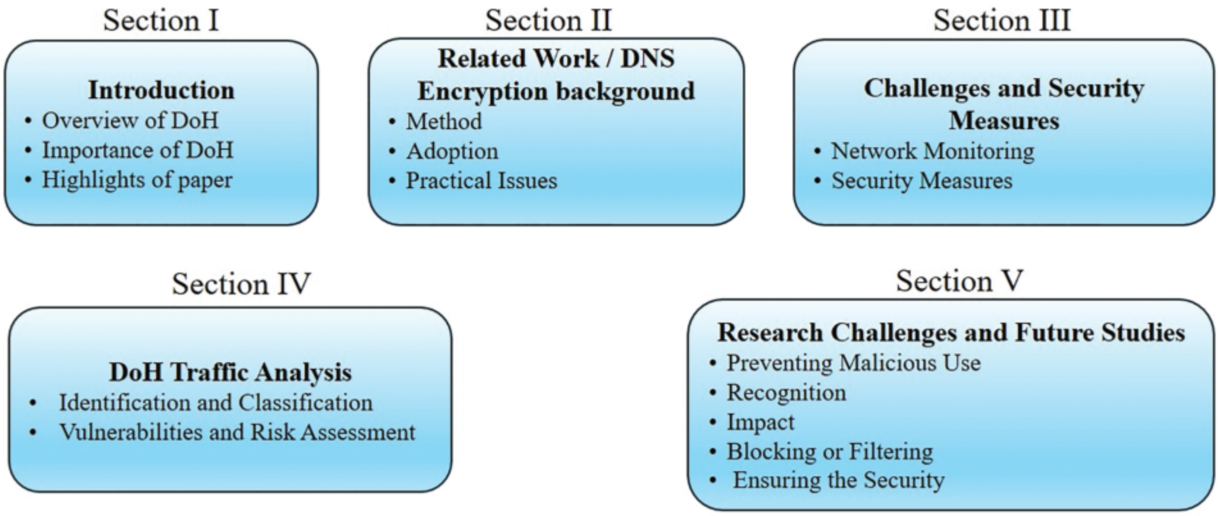


Figure 1: This figure provides a comprehensive overview of the main topics covered in the paper

2 Related Work/DNS Encryption Background

DNS [8] is a crucial protocol for translating human-readable domain names into IP addresses that the system can understand. It operates as a decentralized and hierarchical naming system that connects domain names to IP addresses and is utilized by internet-connected devices. DNS queries are generally transmitted in plaintext, meaning that the contents, including the requested domain name, can be read by anyone who intercepts them. To enhance the traditional DNS protocol's security [9]. DoH has been created, which encrypts DNS queries using the same encryption protocol (HTTPS) used for secure web browsing. This encryption ensures that DNS queries are kept private and cannot be accessed by unauthorized parties. DoH also allows DNS queries to circumvent certain types of internet censorship and filtering, as network administrators cannot easily detect and block the encrypted traffic.

DoH protocol [10] has been officially recognized by the IETF [11] as a standardized way of performing DNS resolution over HTTPS, and the specifications for the protocol are documented in RFC 8484. This makes it easier for different systems and devices to implement the protocol consistently and ensures that DoH provides a standardized level of privacy and security for DNS resolution across the internet.

In RFC 8484, the DoH protocol uses the classic DNS "Wireformat" (the binary format used to encode DNS messages) encapsulated within the HTTPS protocol. The messages are transmitted between the client and server using HTTP GET or POST requests. When a client needs to perform a DNS lookup, it creates a DNS query in the classic "Wireformat" and encapsulates it within an HTTPS request (GET or POST). The request is then sent to a DoH server, which decapsulates the DNS query from the HTTPS request and performs the DNS resolution. The DoH server then encapsulates the DNS response in an HTTPS response and returns it to the client, which decapsulates the DNS response from the HTTPS response and processes the result. Using HTTPS to transmit DNS messages, DoH provides privacy and security for DNS resolution by encrypting the data in transit and preventing eavesdropping and tampering. Additionally, using the classic "Wireformat" for DNS messages, DoH ensures compatibility with existing DNS infrastructure and implementations.

The other approach uses DNS queries, and responses are encoded in the JavaScript Object Notation (JSON) format in RFC 8427 and transmitted as HTTP requests and responses. This allows for more human-readable representations of DNS messages and provides an alternative way to perform DNS resolution using DoH. Many DNS providers support the "Wireformat" of JSON data transfer via HTTPS GET or POST, with many providers supporting the HTTPS GET method.

Popular web browsers like Google Chrome, Edge, and Firefox support DoH. To utilize DoH (DNS over HTTPS) on a client system, proxy software like Cloudflare doh-proxy dnscrypt-proxy, and doh-client can be installed [12,13]. Some network administrators see DoH as a controversial technology, as it can bypass DNS-based content filtering and monitoring policies. However, proponents argue that it provides essential security benefits in preventing DNS hijacking, man-in-the-middle attacks, and other forms of DNS-based surveillance [14]. One area of ongoing research in DoH is improving its performance and scalability, particularly in high-traffic scenarios. Another area of interest is exploring the potential impacts of DoH on network monitoring and filtering and developing new techniques to address these challenges.

In the past, cybercriminals used DNS to communicate with each other secretly. This type of communication, a covert channel, is used to hide the transmission of information from being detected. By exploiting the DNS protocol, attackers can evade security measures and carry out malicious acts. Various techniques are available for detecting DoH traffic [15,16]. One approach is to examine network traffic for HTTPS connections to known DoH endpoints, such as Cloudflare or Google. These DoH endpoints typically use specific domain names, so monitoring network traffic for connections to these domains can help identify DoH traffic. Detecting malicious activity in DoH can be difficult for the current Internet industry's users and responses, which makes inspecting and identifying potentially malicious traffic difficult. However, several methods for detecting malicious activity in DoH include a signature-based approach that detects DoH traffic using pre-defined patterns, such as Uniform Resource Locator (URLs) or headers specific to DoH traffic. This method can detect existing DoH traffic patterns but may struggle to detect new or changed patterns [17]. The behavior-based strategy [18] involves detecting DoH traffic based on network traffic behavior, such as DoH traffic bypassing DNS servers or using non-standard ports. This approach is more versatile and flexible than the signature-based approach but may create more false positives [19]. The machine learning-based approach [20] involves using machine learning algorithms to analyze patterns in network traffic and identify DoH traffic based on these patterns. This approach can be very effective in detecting DoH traffic but requires a large volume of data for training and is more resource-intensive. Table 1 summarizes the advantages and disadvantages of different approaches for detecting DoH traffic and attacks.

Table 1: Challenges and risks of DNS over HTTPS (DoH)

Challenge	Description
Disruption of DNS monitoring and security mechanisms	DoH encrypts DNS queries and responses, making it challenging for network administrators to inspect and filter DNS traffic for malicious activities. Lack of visibility into encrypted DNS traffic can hinder threat detection and response efforts.
Bypassing traditional network security controls	DoH can bypass firewalls and intrusion detection systems (IDS), allowing malicious actors to disguise their activities within encrypted HTTPS traffic. This increases susceptibility to cyber-attacks like command-and-control communication and malware distribution.
Privacy concerns and weaknesses	While DoH aims to improve privacy and security, it allows DNS queries to bypass network-level security measures like firewalls, potentially centralizing DNS requests with single providers and raising concerns about access to private user data. Encryption provided by DoH prevents eavesdropping attacks but does not prevent traffic analysis attacks.
Traffic blending with regular web traffic	Integrating DoH with general HTTPS traffic presents a challenge known as "traffic blending," where DoH queries appear indistinguishable from regular HTTPS traffic, complicating analysis and classification efforts. Advanced techniques like deep packet inspection are necessary to differentiate DoH traffic effectively, balancing network security with user privacy concerns.

DNS tunneling applications such as dns2tcp, DNSCat, and Iodine [21] are software tools that allow users to transport network traffic across DNS requests and responses. This method is used to bypass network security measures that may restrict other sorts of traffic. Yet, DNS tunneling can be used for both legal and harmful purposes. Network administrators can utilize DNS tunneling to remotely administer otherwise inaccessible systems due to security restrictions [22]. Nevertheless, attackers can also use these tools to extract data from a compromised system or to establish a command-and-control channel to remotely control the system or conduct assaults on other systems [23].

2.1 DNS Encryption

The Domain Name System (DNS) initially relied on the User Datagram Protocol (UDP) to resolve domain names to IP addresses, known as DoU (DNS over UDP). However, this method lacked essential confidentiality and integrity guarantees, leaving it vulnerable to eavesdropping and tampering attacks. Additionally, regulatory attempts to mandate Internet Service Providers (ISPs) to block specific web content faced legal challenges due to associated security risks and infringements on free speech. Regulatory requirements also compelled DNS resolver operators to implement parental controls through DNS filtering.

Various encrypted DNS techniques have emerged to address these challenges, including DNS over TLS (DoT), DNS over HTTPS (DoH), and DNSCrypt. These methods enable secure communication between clients and recursive DNS resolvers by encrypting DNS traffic. Recent advancements have witnessed widespread support for DoH across desktop web browsers, mobile clients, and operating systems. DoH and DoT protocols establish Transport Layer Security (TLS) sessions between clients and resolvers, ensuring authenticated and secure connections. The adoption of DoH has surged, with public services such as Cloudflare and NextDNS [24] offering DoH integration, particularly in browsers like Firefox, where Cloudflare is the default resolver [25].

While specific organizations enforce privacy policies to prevent user tracking, others may aggregate user traffic patterns for their business interests. Generally, DNS encryption involves encapsulating query and response content utilizing cryptographic techniques to encrypt packet contents between clients and resolvers within an upper-layer protocol.

This evolution in DNS encryption signifies a significant leap forward in enhancing internet security and privacy, ensuring the confidentiality and integrity of DNS communications in an increasingly interconnected digital landscape.

2.2 Overview of Standard DNS Encryption Protocols

DNS encryption techniques enhance privacy and security by safeguarding Domain Name System (DNS) queries from unauthorized access and monitoring. Presently, there are three recognized DNS encryption methods, each utilizing a distinct upper-layer protocol: DoT, DoH, and DoQ. These methods encapsulate DNS within encryption-enabled layers—namely, TLS, TLS with HTTP (i.e., HTTPS), and QUIC.

DNS over TLS (DoT) was the initial standardized protocol for DNS encryption, with its RFC [17] published in 2016. It uses the Transmission Control Protocol (TCP) transport layer and TLS to encrypt DNS queries and responses. When performing lookups, the client starts by creating a TCP connection to the DoT port TCP/853 on the targeted DoT-enabled resolver. First, a TLS connection is established using the standard TLS handshake process to exchange cryptographic keys, nce this TLS session is set up, the client can perform DNS lookups encrypted by TLS through the resolver's DoT port TCP/853. However, despite its security benefits, DoT encounters several practical challenges that could restrict its adoption. One issue is that firewall appliances are likely to block the port TCP/853 that is used for DoT services because it is not yet widely acknowledged by the security community.

While the content of queries and responses is encrypted, eavesdroppers can obtain encrypted DNS packets relatively quickly (compared to DoH and DoQ, where a mix of traffic is exchanged) by filtering TCP/853 and performing statistical analysis to infer their embedded contents. Another drawback of DoT is that it necessitates support from application developers and hardware manufacturers. Without their support, users might remain unprotected. Additionally, DoT is less resilient to packet losses compared to DoH and DoQ [26].

The imperative for application developers and hardware manufacturers to endorse DNS over TLS (DoT) introduces practical concerns that could impede widespread adoption, potentially leading to fragmentation in the DNS landscape. Despite the enhanced security and privacy benefits offered by encrypting DNS traffic during transmission, the efficacy of DoT relies heavily on comprehensive support across diverse applications and hardware platforms. The risk of a fragmented ecosystem arises if DoT is not universally embraced, leaving users of unsupported applications or devices vulnerable to security threats as their DNS queries persist in plaintext. Adoption barriers may emerge if developers and manufacturers do not uniformly implement DoT support, hindering users from accessing the security advantages of encrypted DNS. This non-uniform adoption could result in inconsistencies in protecting DNS traffic, with some applications or devices utilizing the secure DoT channel. In contrast, others persist with traditional, unencrypted DNS, creating an uneven security landscape. In such a scenario, raising user awareness and education becomes crucial to emphasize the importance of utilizing applications and devices that support DoT, preventing inadvertent compromises to privacy and security [27].

DNS over HTTPS (DoH) [18] was standardized in 2018 to address the DoT's practical shortcomings. It uses the common HTTPS protocol (TLS with HTTP) to encapsulate DNS data, transmitting it through the service port TCP/443. DoH is recommended since it offers compliance with current security standards and is the default protocol for many browsers, including HTTPS. DoH is the best privacy solution since it integrates DNS traffic with other HTTPS applications. It also benefits from upcoming HTTPS efficiency and security enhancements. Because of these advantages, DoH is currently the most extensively used DNS encryption method [5].

DNS over QUIC: (DoQ) is a proposed protocol for encrypting DNS requests that use the QUIC protocol built on top of the UDP transport layer [19]. DoQ aims to improve the performance of encrypted DNS compared to DNS over TCP (DoT) and DoH, which can be slower due to the required TCP and TLS handshakes and acknowledgment mechanisms. DoQ is designed to be faster and more efficient. DoQ was first introduced by Google in 2017 as an Internet draft to improve the performance of encrypted DNS, but it has not yet been officially finalized as an RFC [19]. By using zero-RTT (Round-Trip Time) handshakes and multiplexing data streams, DoQ enables faster and lighter encrypted communications. Studies have shown that QUIC outperforms HTTPS in response quality metrics such as page load times. However, like DoT, DoQ uses dedicated service ports that are not yet widely recognized by security systems, which means that its traffic may be blocked by firewalls during transmission [28].

2.3 Emerging Trends in DNS Encryption Adoption

The adoption of DNS encryption, propelled by growing concerns over privacy and security, has witnessed significant advancements in recent years. Key stakeholders, including Since 2019, major cloud providers like Cloudflare and Google have supported DNS encryption. Many other providers, such as AdGuard, Alibaba, Cisco, Comcast, and Quad9, have followed this initiative, expanding encrypted DNS infrastructure.

Public resolvers now boast a robust ecosystem, with an increasing number of DNS over TLS (DoT) and DNS over HTTPS (DoH) enabled servers available worldwide. AdGuard's experimental support for DNS over QUIC (DoQ) signifies ongoing innovation in this domain, promising even more secure and efficient DNS communication channels.

Despite these strides, challenges persist, particularly regarding data monopolization and regulatory opposition. Concerns raised by groups such as ISPA, the UK's Internet Services Providers Association underscore the need for a balanced approach to DNS encryption adoption, addressing both security imperatives and regulatory compliance. User acceptance remains a critical factor in driving widespread adoption. While major operating systems and internet browsers have integrated DNS encryption features, user reluctance persists. Addressing usability concerns and streamlining integration processes are imperative to accelerate adoption rates. Performance analysis plays a pivotal role in assessing the efficacy of DNS encryption solutions. As encrypted DNS introduces additional communication overheads compared to plaintext DNS, empirical evaluation becomes essential to gauge its impact on various network environments and application scenarios.

Hounsel et al. [29] conducted a study to assess the impact of different DNS options (plaintext DNS, DoH, and DoT) on web page load times across various networks, including cellular 3G, lossy cellular 4G, and campus wired networks. Their findings revealed that the load times for all three protocols were nearly identical in an ideal university network environment, showing statistical differences approaching zero seconds. However, in 3G networks, plaintext DNS outperformed DoT and DoH, while in lossy 4G networks, DoT exhibited the best performance, followed by DoH and plaintext DNS. The authors attributed these differences to TCP (used by DoT and DoH) having shorter timeout thresholds compared to UDP (used by plaintext DNS).

Borgolte et al. [30] investigated the variations in page load times between plaintext DNS and DNS over HTTPS (DoH) on 4G and campus network scenarios. Three open resolvers from Google, Cloudflare, and Quad9 were tested. The results demonstrated that, when compared to other university networks, only Cloudflare's DoH solution had the most feasible load times. However, other combinations resulted in significant delays, such as up to 5 s for DoH using the Quad9 resolver under the 4G network. The authors also observed that network conditions susceptible to loss and suboptimal provider choices could amplify the performance disparities between DNS and DoH protocols.

2.4 Practical Challenges in DNS Encryption

Despite the significant advantages of encrypted DNS, its implementation is challenging. Practical issues and security vulnerabilities can impact the effectiveness and reliability of encrypted DNS solutions, potentially exposing users to risks and compromising the integrity of DNS communications. Understanding these challenges is essential for mitigating risks and ensuring the robustness of encrypted DNS deployments.

This section explores the security vulnerabilities and practical issues with encrypted DNS protocols. By identifying and addressing these challenges, stakeholders can enhance the security posture of their DNS infrastructure and promote the widespread adoption of encrypted DNS technologies.

However, despite the protective measures afforded by these encryption protocols, the potential for privacy leakage persists, particularly in scenarios involving compromised resolvers [31].

2.4.1 Privacy Risks Posed by Compromised Recursive Resolvers

Unlike authoritative name servers, Recursive resolvers occupy a critical position in the DNS resolution process, serving as intermediaries between clients and authoritative servers. This intermediary role grants recursive resolvers the capability to compile comprehensive profiles of users based on their DNS queries and responses. In the event of a resolver compromise, malicious actors gain access to sensitive user information, posing a significant risk to privacy.

While resolver compromise is not exclusive to encrypted DNS environments and has historically been observed in plaintext DNS systems, the emphasis on privacy protection in encrypted DNS protocols heightens the importance of resolver security. Protecting user privacy becomes a primary objective in encrypted DNS, necessitating robust security measures to mitigate the risks associated with compromised resolvers [14].

Siby et al. [26] highlighted that payload manipulation by compromised resolvers is relatively common, even with encrypted DNS protocols such as DNS over TLS (DoT) and DNS over HTTPS (DoH). They conducted over seven million DNS lookups aimed at thousands of DoT/DoH-enabled DNS resolvers. Their results indicated that over 1.5% of the responses were manipulated, according to their ground-truth records of domain names and corresponding IP addresses. This finding underscores the importance of considering security measures beyond encryption when implementing DNS security protocols.

Rivera et al. [32] introduced a privacy-preserving approach utilizing an extended Berkeley Packet Filter (eBPF). This mechanism enables users to distribute their DNS queries randomly across a set of resolvers. Doing so mitigates the risk of a compromised resolver exposing a client's entire history of query records. This method enhances user privacy and security when interacting with DNS resolvers. Invalid SSL certificates in the context of DNS over TLS (DoT) and DNS over HTTPS (DoH) resolvers pose privacy risks to users during the SSL handshake process, where certificates are presented as proof of identity. The reasons for certificate invalidity varied, including non-existent issuers, self-assigned certificates, expired certificates, and expired windows It is noteworthy that certain resolvers with invalid certificates may not have been meant for general public usage. They can be the abandoned servers from temporary university network experiments.

Lu et al. [33] reported that a significant portion (25%) of the DNS over TLS (DoT) servers they examined had invalid SSL certificates. These invalid certificates pose potential privacy risks to clients because they cannot be verified as trusted entities. This lack of verification may lead to security vulnerabilities and compromise user privacy during encrypted DNS sessions.

Based on real-world observations, service operators must ensure the validity of SSL certificates while providing public DNS services that are encrypted. This practice helps maintain trust, protect user privacy, and avoid potential security vulnerabilities during encrypted DNS sessions.

2.4.2 Risks of Fallback Attacks in DNS Encryption Protocols

By default, clients generally use the "opportunistic" or "automatic" mode to form encrypted connections with resolvers through available DNS encryption protocols. In this mode, if both parties cannot agree on an encryption protocol, DNS lookups revert to plaintext. However, malicious actors can exploit this by compelling clients to perform DNS lookups in plaintext as part of a fallback or downgrade attack strategy.

Fallback attacks leverage the fact that servers running updated or secured protocols like DNS over HTTPS (DoH) and DNS over TLS (DoT) may still support older, less secure protocols such as plaintext DNS to maintain backward compatibility. During these attacks, malicious actors may employ methods like man-in-the-middle attacks to fabricate false negotiations between the client and server. leading to using a less secure protocol in subsequent communications. The DNS encryption options for user applications list different options for users to encrypt their DNS communications are summarized in Table 2.

Regarding the feasibility of fallback attacks, Huang et al. [34] identified four techniques that could enable such fallback DNS cache poisoning, TCP connection reset, DNS traffic interception and TCP traffic manipulation The authors tested these techniques on major browsers like Chrome and Firefox. They found that all tested browsers were vulnerable to at least one of these fallback methods despite variations in response patterns.

Table 2: "DNS encryption options for user applications" lists different options for users to encrypt their DNS communications

Options	Description
Off	Plain text without attempting to apply encryption for DNS communications.
Opportunistic/Automatic [35]	Apply encryption, if possible, by both client and server; otherwise, use plaintext DNS (if no encryption protocol is available/possible).
Strict	Apply specified encrypted DNS protocols, and do not use plaintext DNS.
DNS over TLS (DoT)	Use Transport Layer Security (TLS) to encrypt DNS queries and responses over port 853.
DoH	Use HTTPS to encrypt DNS queries and responses over port 443.
DNSCrypt	Use a custom DNS encryption protocol to encrypt DNS queries and responses.
Anonymized DNS	Use encryption and routing techniques to obscure DNS queries and responses from eavesdroppers.

Therefore, the authors recommend that application developers reconsider their encryption policies, such as notifying users if the plaintext is chosen, instead of solely relying on the "opportunistic" mode as the default option.

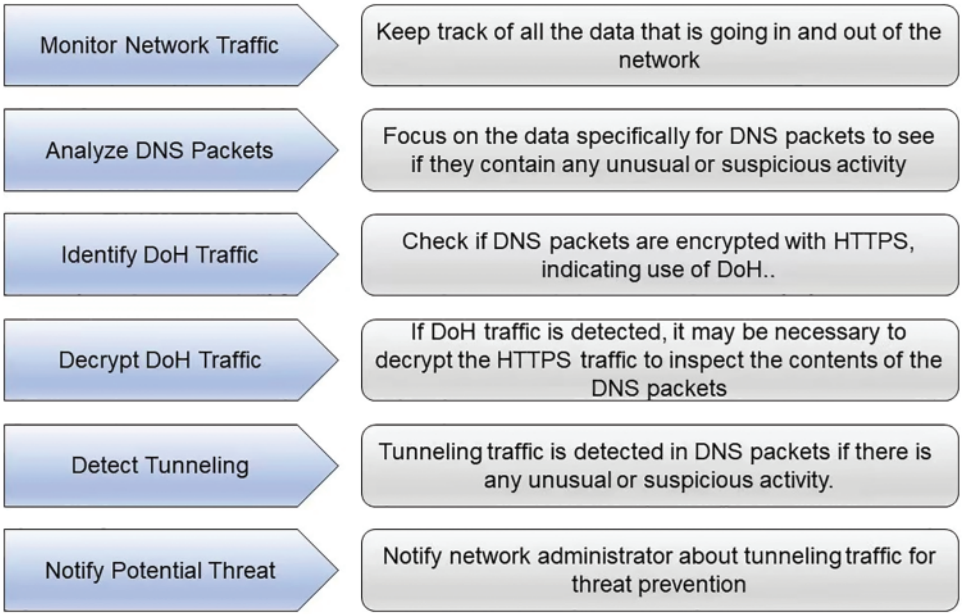
The adoption of DNS encryption has been gaining momentum, with major cloud providers like Google and Cloudflare leading the way since 2019. Other providers such as AdGuard, Alibaba, Cisco, Comcast, and Quad9 have followed suit [35,36]. There are currently at least seven DoT-and DoH-enabled public resolvers available online, per technical reports [5]. However, the adoption is still dominated by a few major service providers, raising concerns about data monopolization. Despite the growing adoption, there is also opposition to DNS encryption. The UK Internet Services Providers' Association (ISPA) has also expressed opposition to DNS encryption, arguing that it can circumvent existing filtering requirements and compromise internet safety standards [37]. DoH features have been integrated into the latest versions of major operating systems, including Windows, macOS, Linux, iOS, and Android. Likewise, popular internet browsers, including Chrome and Firefox, now support DoH [38], and Opera provides DNS encryption options for users. These options typically come in three modes: "Off," "Opportunistic" (or "Automatic"), and "Strict".

In the "Off" mode, DNS lookups are conducted in plaintext. The "Opportunistic" mode allows the client and its resolver to negotiate a DNS encryption protocol available to both parties. If no agreement is reached, the data exchange defaults to plaintext. In the "Strict" mode, DNS lookups can only be performed via a specific encryption protocol specified by the user [35]. The growing adoption of DNS encryption by user applications is a promising sign for the future of secure and private internet browsing, as depicted in Table 3.

Table 3: Summarization of various DNS encryption methods with their availability/suitability

Encryption method	Availability/Suitability
Off	Not secure
Opportunistic/Automatic	Basic security
Strict	Enhanced security
DoT	Secure, but may face firewall and eavesdropping challenges
DoH	Secure, integrates with HTTPS, Enhanced security
DNSCrypt	Secure, Offers privacy
Anonymized DNS	Secure, Offers anonymity

Fig. 2 shows the steps that can be taken to detect DoH tunneling in network traffic. First, to monitor network traffic, identify potential DoH traffic, confirm it as DoH traffic, analyze the packets for abnormal behavior, compare the traffic to known DoH tunneling profiles, and take appropriate action to mitigate the threat. We explore various methods to detect malicious DNS tunneling activities within DoH traffic.



Keep track of all the data that is going in and out of the network

Focus on the data specifically for DNS packets to see if they contain any unusual or suspicious activity

Check if DNS packets are encrypted with HTTPS, indicating use of DoH..

If DoH traffic is detected, it may be necessary to decrypt the HTTPS traffic to inspect the contents of the DNS packets

Tunneling traffic is detected in DNS packets if there is any unusual or suspicious activity.

Notify network administrator about tunneling traffic for threat prevention

Figure 2: Steps for detecting DoH tunneling in network traffic

3 Challenges and Security Measures for DNS over HTTPS (DoH)

Adopting DNS over HTTPS (DoH) introduces various challenges that organizations must navigate to ensure the security and integrity of their network infrastructure. This section explores these challenges in-depth, addressing issues such as the encryption of DNS queries and responses, which complicates traditional monitoring and security mechanisms. Additionally, we delve into the potential risks associated with DoH bypassing network security controls and its implications for threat detection and response efforts. Alongside these challenges, we discuss essential security measures and strategies to mitigate the risks posed by DoH adoption. These measures include enhancing network monitoring capabilities, developing advanced tools for inspecting encrypted DNS traffic, integrating firewalls and intrusion detection systems, and ensuring compatibility with DoH protocols. By understanding these challenges and implementing effective security measures, organizations can bolster their defenses and safeguard their networks against emerging cyber threats related to DNS over HTTPS.

3.1 DoH Monitoring Challenges

Deploying DNS over HTTPS (DoH) introduces various challenges and risks that organizations need to address to ensure the security and integrity of their network infrastructure and data. One primary challenge is the potential disruption of existing DNS monitoring and security mechanisms. Since DoH encrypts DNS queries and responses, it complicates the ability of network administrators to inspect and filter DNS traffic for malicious activities, such as malware communication or unauthorized data exfiltration. This lack of visibility into encrypted DNS traffic can hinder threat detection and response efforts, leaving networks vulnerable to cyber threats.

Another challenge is the potential for DoH to bypass traditional network security controls, including firewalls and intrusion detection systems (IDS). Malicious actors could leverage DoH to disguise their activities within encrypted HTTPS traffic, making it difficult for security devices to detect and block malicious behavior effectively. This can increase susceptibility to various cyber-attacks, such as command-and-control communication or malware distribution, which exploit the encrypted nature of DoH traffic to evade detection [39].

DoH is a protocol that encrypts DNS queries and responses using the HTTPS protocol. It is intended to improve the privacy and security of DNS traffic, which is typically sent in plaintext and can be intercepted and manipulated by attackers. However, while DoH has some advantages, it has potential privacy weaknesses. One of the main concerns with DoH is that it allows DNS queries to bypass network-level security measures like firewalls and content filters. This can make monitoring and controlling network resources more difficult for organizations [40]. Another issue is that DoH might permit DNS requests centralized with a single provider, like Google or Cloudflare. This might give these providers access to private data about users' browsing patterns, which they might use for marketing or other purposes [41]. Encryption, such as that provided by DoH, can help prevent eavesdropping attacks by making it difficult for attackers to read the contents of DNS queries. However, encryption alone does not prevent traffic analysis attacks. Even if an attacker cannot read the contents of the queries, they can infer information about the user's browsing activity by analyzing the size and timing of DNS queries [42].

To enhance privacy, a DNS protocol known as Extension Mechanism for DNS (EDNS) padding was developed [43]. EDNS padding is a technique that involves adding random data to DNS queries to make them all the same size. This makes it much more difficult for an attacker to infer anything about the query from its size because all queries are the same size. Random padding also helps to prevent timing attacks since the timing of a query is no longer correlated with its size. One of the potential attacks that makes use of side-channel data is website fingerprinting. Research has shown that website fingerprinting attacks against DoH connections can be successful, especially if the attacker has prior knowledge of the websites being accessed. However, the effectiveness of these attacks is determined by several factors, including the size and diversity of the websites being accessed and the specific implementation of the DoH protocol. The foundation of fingerprinting attacks is that each website connection creates a distinct sequence of packet sizes, which the adversary may use to deduce the transmitted and encrypted information. Various countermeasures have been proposed to mitigate the risk of website fingerprinting attacks in DoH, including padding the encrypted packets to make them more uniform and introducing dummy traffic to disguise the actual traffic. Ongoing research is needed to determine the effectiveness of these countermeasures and to develop new techniques for defending against website fingerprinting attacks in DoH.

Sun et al. [42] studied the downgrade privacy attack, which blocks a browser's encrypted DoH connection and forces it to use unencrypted DNS instead. The researchers tested six different browsers that support DoH, employing four different attack vectors: DNS traffic interception, DNS cache poisoning, TCP traffic interception, and TCP reset injection. TCP traffic interception and TCP reset injection. Because there are no user notifications and relaxed reconnections, the evaluation identifies that any combination of browser and attack vector results in a successful attack. However, the assault is difficult to detect. The impact of a downgrade attack could be minimized by providing sufficient warning of lost privacy; however, none of the browser providers intend to implement it.

3.1.1 DNS over HTTPS (DoH) Blends in with Regular Web Traffic

In the evolving landscape of secure online communication, integrating DNS over HTTPS (DoH) with general HTTPS traffic introduces a nuanced challenge known as "traffic blending." DoH, serving as a protocol to enhance privacy by encrypting DNS queries within the secure confines of HTTPS, shares a crucial characteristic with regular HTTPS traffic—they both utilize the ubiquitous port 443 for communication. This commonality renders them indistinguishable at the network level based solely on port numbers, creating a visual uniformity that conceals the distinctive nature of DoH queries.

The traffic blending challenge arises because when DoH queries traverse the network, they adopt the encrypted guise of HTTPS traffic. This blending effect presents a considerable obstacle in isolating and analyzing DoH traffic separately from general HTTPS communication. The uniform appearance of DoH queries alongside a vast volume of HTTPS traffic on port 443 complicates the efforts of security analysts and network administrators to discern the specific characteristics of DoH traffic.

The implications of traffic blending are multifaceted. Firstly, the complexity introduced in network traffic analysis necessitates advanced techniques for accurate identification and classification. Security monitoring systems, reliant on distinguishing between various types of traffic, may encounter challenges in effectively isolating DoH queries and distinguishing them from regular HTTPS traffic. This reduced visibility into the distinct features of DoH queries hampers the overall security posture and introduces potential misclassifications. As the adoption of DoH continues its upward trajectory, security systems must undergo adaptation to address the intricacies of traffic blending. Incorporating advanced traffic analysis techniques, such as deep packet inspection, is imperative for security systems to differentiate between DoH and general HTTPS traffic [44]. However, this adaptation must be approached with a nuanced consideration of user privacy, striking a delicate balance between ensuring network security and respecting user privacy concerns associated with deep packet inspection. Traffic blending encapsulates the challenge posed by the seamless integration of DoH queries with general HTTPS traffic, making it arduous to isolate and analyze DoH traffic distinctly. This challenge underscores the evolving dynamics of secure communication protocols and emphasizes the need for adaptive security measures in the face of increasing DoH adoption.

3.1.2 Phishing

Phishing attacks [45] typically involve sending fraudulent emails, text messages, or social media messages that appear to be from a legitimate source, such as a bank, an e-commerce website, or a social media platform. DoH can bypass traditional DNS filtering and security mechanisms, allowing attackers to host phishing websites on domains not yet detected or blocked by security tools. This means that phishing websites may not be identified as malicious or suspicious by traditional DNS-based security measures, making it easier for attackers to lure victims into clicking on malicious links or providing sensitive information. By using DoH, attackers could potentially hide the valid IP addresses of their phishing website or conceal the DNS queries associated with their phishing campaign. Another potential risk associated with DoH is that attackers could exploit the trust that users have in HTTPS connections to make their phishing websites or communications appear more legitimate.

3.1.3 Using DoH for C2 (Command and Control) Communication

C2 traffic is crucial to a cyber-attack because it allows the attacker to control the compromised device and perform malicious activities remotely. Using DoH for C2 communication can make it more difficult for security teams to detect and remediate compromised devices because the traffic is encrypted and can be disguised as legitimate HTTPS traffic [45]. This can help cybercriminals avoid detection by security tools that rely on inspecting network traffic for malicious activity. Overall, the use of DoH for C2 communication emphasizes the importance of a multi-layered defense strategy that includes network monitoring, endpoint protection, and threat intelligence to detect and mitigate potential threats. To reduce the risk of successful attacks, organizations must also implement best practices such as regular software updates, strong password policies, and employee education [18].

There are serious cybersecurity issues with integrating DNS over HTTPS (DoH) for Command and Control (C2) communication, especially regarding the encryption of DoH traffic. Encryption, intended to improve user privacy, becomes a double-edged sword because it gives threat actors involved in C2 activities a covert communication channel. DoH traffic is encrypted, which makes it difficult for security teams to detect and mitigate. When used with DoH, conventional techniques for examining DNS traffic patterns or identifying recognized malicious indicators become less valuable, limiting insight into the details of the communication and making it more challenging to detect compromised devices promptly.

The challenges continue into the mitigation phase when security teams find it difficult to react appropriately and quickly to threats identified due to the hidden contents of DoH traffic. This creates a possible opening in the mitigation process that might let hostile actors keep prolonged control over infected devices. Since the secure communication channel makes it difficult for security teams to intervene quickly, the encrypted nature of DoH may allow threat actors to carry out protracted malicious activities without detection or interference.

A recurring theme is the precarious equilibrium between the need to uphold strong security measures and user privacy, which encryption seeks to protect. Businesses implementing DoH face the difficult task of protecting user privacy while ensuring they have the control and visibility needed to identify security threats and take appropriate action. A significant implication of DoH for C2 communication is the ability to evade conventional security measures. This is because it can circumvent signature-based detection techniques used by security systems, enabling threat actors to move undetected through security perimeters. Because threat actors use encrypted channels to conceal their activities, the integration of DoH in C2 operations adds to the growing sophistication of malware. DoH gives bad actors easier access to a dynamic and adaptable C2 infrastructure, which makes it more difficult for security teams to find and block malicious domains proactively. DoH-based C2 communication is encrypted, which presents significant challenges for incident response teams because it obscures essential information necessary for efficient incident response and hinders forensic analysis.

Within the cybersecurity community, cooperation is needed to address these issues. To create cutting-edge solutions and best practices, industry stakeholders must collaborate, including security vendors, researchers, and standards organizations. To strike a balance between user privacy and open security practices, regulatory bodies may decide to review standards and compliance requirements in light of the growing popularity of encrypted communication channels like DoH. Continuous research and development is necessary to keep ahead of evolving cyber threats, and innovation in this quickly evolving environment depends on cooperation between the research community and industry practitioners. A proactive and cooperative approach to research, development, and regulatory considerations will be crucial in managing the complexities of DoH for C2 communication and reducing any potential risks related to this encryption technology in the context of cyber threats.

3.2 Implementing Enhanced Security Measures

This section discusses the challenges organizations face when deploying DNS over HTTPS (DoH) and explores strategies to overcome disruptions in existing DNS monitoring and security mechanisms. By addressing these challenges, organizations can ensure the security and integrity of their network infrastructure and data.”

3.2.1 DNSSEC (Domain Name System Security Extensions)

DNSSEC [46] is a set of protocols that provide data origin authentication and data integrity for DNS data. DNSSEC was created to address vulnerabilities in the DNS system that attackers can use to launch DNS spoofing attacks, also known as DNS cache poisoning attacks. An attacker can use DNS spoofing to modify DNS records in a DNS cache to redirect users to malicious websites or intercept their communications. DNSSEC protects against DNS spoofing attacks by allowing DNS clients to use digital signatures to validate the authenticity of DNS records. DNS records signed with DNSSEC can be verified by DNS clients using a chain of trust that begins with a trusted root key and extends to the authoritative DNS server for the domain in question. In terms of interoperability. DNSSEC adds cryptographic signatures to DNS records, allowing DNS clients to verify the authenticity of the DNS data they receive. DNSSEC achieves this by introducing new resource record types, such as Resource Record Signature (RRSIG), Key (DNSKEY), and Delegation Signer (DS). When a DNS resolver receives a DNSSEC-enabled query, it can request that the DNS server provide signed DNS records and the public key used to sign them. The resolver can then use the public key to verify the signature and confirm the authenticity of the DNS data [47].

3.2.2 Query Name Minimization

Query Name Minimization [48] can be used to improve DoH query privacy. When DoH is used, the DNS query is encrypted and sent to a remote server over HTTPS. This helps to protect the query’s privacy and integrity while it is in transit. However, once the query reaches the remote server, the server may still be able to log or analyze the query, revealing sensitive information about the user. The amount of information disclosed in each query can be reduced by using Qualified Name (QNAME) minimization, which can help to protect user privacy even more when QNAME minimization is used with DoH, the recursive resolver only sends the minimum needed information to the remote server to resolve the query. This may help to keep the user’s identity from being revealed to the remote server by preventing it from seeing the entire query name. Overall, QNAME minimization with DoH can provide additional privacy protections for DNS queries, particularly crucial in today's increasingly privacy-conscious online environment [49]. The positive and negative impacts of DoH on internet privacy and security are shown in Fig. 3.

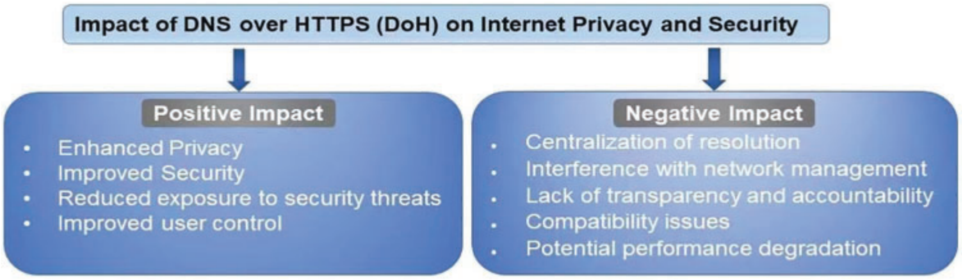

Impact of DNS over HTTPS (DoH) on Internet Privacy and Security
Positive Impact
Enhanced Privacy
Improved Security
Reduced exposure to security threats
Improved user control
Negative Impact
Centralization of resolution
Interference with network management
Lack of transparency and accountability
Compatibility issues
Potential performance degradation

Figure 3: This figure illustrates the potential positive and negative impacts of DoH on cybersecurity

3.2.3 SSL Certificates

SSL certificates are digital files that securely connect cryptographic keys to an organization's information, including its hostname, server name, domain name, and organizational details such as uniqueness and geographical location. These certificates ensure secure communication between web servers and browsers, safeguarding sensitive data transmissions like logins and financial transactions. Upon installation on a web server, SSL certificates establish a secure connection, denoted by the switch from HTTP to HTTPS in the website address. Depending on the certificate type and browser, users may see visual indicators like padlocks or green bars, signifying a secure connection. SSL certificates, also known as public-key cryptography certificates, rely on a pair of keys—a private key known only to the server and a public key available to the public—to encrypt and decrypt messages. This asymmetric encryption ensures that only the intended recipient can decrypt the messages, enhancing security. The advantages of SSL certificates include building customer trust, improving search engine rankings, protecting against phishing attacks, and avoiding warnings from search engines like Google. SSL certificates are essential for safeguarding online transactions and enhancing website security [50].

DoT [47] can also secure DNS communication by encrypting messages exchanged between users and resolvers. DNS messages are encapsulated in a TLS tunnel with DoT, ensuring data security while in transit and reducing the risk of man-in-the-middle attacks.

4 Exploring DoH Traffic Analysis and Security Assessment

This section delves into sophisticated methods for recognizing and categorizing DNS over HTTPS (DoH) traffic within network environments. These advanced techniques include traffic analysis, machine learning algorithms, statistical modeling, and behavioral profiling. By employing these methods, we aim to accurately classify DoH traffic, such as DoH and non-DoH, benign and malicious. This classification process is crucial for network administrators and security professionals to manage and secure networks implementing DoH protocols. By thoroughly exploring these classification methods, we gain valuable insights into the intricate nature of DoH traffic and potential security implications [5].

4.1 DoH Traffic Identification and Classification Methods

This topic delves into the advanced methodologies for recognizing, classifying, and categorizing DNS over HTTPS (DoH) traffic within network environments. It encompasses a range of innovative techniques, including traffic analysis, machine learning algorithms, statistical modeling, and behavioral profiling, to accurately identify DoH communication patterns amidst diverse network traffic. The primary objective is to classify DoH traffic into different categories, such as DoH and non-DoH, benign and malicious, based on its characteristics, such as source, destination, behavior, and potential security implications. These classification methods are pivotal for network administrators and security professionals in effectively managing and securing networks that implement DoH protocols. “Through our investigation, we’ll uncover the interesting findings and new methods discussed in the following papers:”

Mitsuhashi et al. [51] introduced a novel approach for identifying malicious DNS tunneling activity by analyzing DNS over HTTPS (DoH) traffic using a hierarchical machine-learning classification approach. They provide a comprehensive overview of DNS tunnels, detection methods, and evaluation metrics aimed at accurately distinguishing between legitimate and malicious DoH traffic. The experimental results of their proposed method demonstrate high levels of effectiveness, achieving a 99.81% accuracy rate for DoH traffic filtering, a 99.99% accuracy rate for detecting suspicious DoH traffic, and a 97.22% accuracy rate for identifying malicious DNS tunnel tools. This highlights the robustness of their approach in accurately identifying and mitigating DNS tunneling threats within network environments.

Vekshin et al. [52] developed a machine-learning approach to recognize DNS over HTTPS (DoH) traffic and identify the DoH client. They gathered a detailed dataset, selected important features like packet size, timing, domain name patterns, traffic volume, protocol headers, and encrypted payload content, and conducted time-series analysis. Their models achieved over 99% accuracy in recognizing DoH communication and correctly identifying the DoH client. This method shows promise in improving network security and privacy for systems using DoH.

Singh et al. [53] discussed using machine learning algorithms to detect malicious activities at the DNS level in DoH environments. The authors use a dataset (CIRA-CIC-DoHBrw-2020) and extract several features to develop a robust model. Several machine learning classifiers such as Naive Bayes, Logistic Regression, Random Forest, K-Nearest Neighbor, and Gradient Boosting are used to evaluate the performance. The Random Forest and Gradient Boosting classifiers outperformed other classifiers, with accuracy rates of 99.89% and 99.87%, respectively. The Naive Bayes classifier had the lowest accuracy rate, at 91.47%. The Logistic Regression and K-Nearest Neighbor classifiers had accuracy rates of 98.69% and 99.83%, respectively. The study found that machine learning can effectively identify malicious activity in encrypted web traffic.

Kwan et al. [54] created a threshold-based technique to distinguish between benign DoH communications and DoH tunneling that takes into account packet size, packet rate, and throughput.

Their method of identifying DoH tunneling produced by the “dnstt” tool was 100% accurate [3]. Additionally, the study showed that DNS tunneling could only avoid their detection technique if its rate was notably decreased by a factor of 27.

Lu et al. [33] utilized time-series modeling with the Hodrick-Prescott (HP) filter to analyze response sizes in DoT and DoH traffic from benign and malware-infected hosts. Their analysis revealed unique patterns in the time-series signals of packet sizes, enabling the identification of hosts engaged in Command and Control (C&C) communications and the classification of their respective malware families [55].

MontazeriShatoori et al. [56] explored the use of machine learning to detect DoH traffic. They tested five machine learning methods to find the best ones for spotting DoH activity, achieving an accuracy rate of over 99.9%. Additionally, they managed to identify the specific applications used for DoH communication. The authors trained a classifier to accurately recognize DoH traffic and its associated applications by analyzing data and behaviors. Overall, this paper shows how machine learning can effectively analyze encrypted traffic, highlighting the need to adapt security tools for dealing with DoH challenges.

4.2 DoH Protocol Vulnerabilities and Risks Assessment

DoH Protocol Vulnerabilities and Risks Assessment involves evaluating the potential weaknesses and security risks associated with the DNS over HTTPS (DoH) protocol. This assessment typically includes analyzing the protocol's design, implementation, and deployment to identify vulnerabilities malicious actors could exploit. The goal is to understand the threats and risks posed by using DoH for DNS resolution, including privacy concerns, potential abuse scenarios, and implications for network security. This assessment helps organizations and stakeholders make informed decisions regarding adopting and implementing DoH to mitigate identified risks effectively.

Hynek et al. of this study [3] analyzed the growing problem of DoH protocol abuse. They identify the sorts of abuse facilitated by DoH and the possible threats for internet users and networks based on a comprehensive analysis of a huge dataset of DoH traffic. The authors highlight the risk of malicious actors abusing DoH for phishing, malware distribution, and other illegal activities, and they offer many strategies to prevent or mitigate such abuse. The authors recommend that DoH providers implement secure and transparent policies to prevent abuse and that internet service providers (ISPs) and network operators monitor and restrict the use of DoH in their networks to prevent malicious activities. The article provides valuable insights into the issue of DoH abuse and the measures that can be taken to prevent it.

The "DoH Study" by The Internet Corporation for Assigned Names and Numbers (ICANN)'s Security and Stability Advisory Committee (SSAC) [57] examines the security and privacy implications of resolving domain names using DoH. DoH is a new DNS security approach that encrypts DNS requests and responses between client and server to prevent eavesdropping and tampering. The report provides a detailed technical analysis of how DoH works and discusses the potential advantages and disadvantages of using DoH for DNS resolution. It emphasizes the potential for DoH to improve the privacy and security of DNS transactions. It also points out challenges such as the possibility of concentrating DNS resolution in the hands of a few providers, reducing competition, and increasing the risk of a single point of failure. The report suggests more DoH research and investigation, such as investigating the compatibility of different DoH implementations and the security and privacy implications of deploying DoH in various deployment circumstances. Overall, the study is an excellent resource for anyone interested in learning about the security and privacy concerns of utilizing DoH to protect the DNS.

Hynek et al. [43] analyzed how the DoH protocol is implemented in Firefox and Chrome browsers and evaluated the depth of information exposed through packet-level data observation and analysis. The studies found that even though encrypted communication leaks private information, it can be misused. The authors trained a machine learning classifier and discovered that it is possible to infer individual domain names only from the captured encrypted DoH connection with surprisingly high accuracy, up to 90% on HTTP 1.1 and up to 70% on HTTP 2. To address the protocol's privacy weaknesses, the authors recommend adding padding.

4.3 Behavioral Profiling and Analysis of Encrypted DNS Traffic

Behavioral profiling and analysis are critical in understanding encrypted DNS (Domain Name System) traffic patterns and characteristics within network environments. This section explores the methodologies and techniques used for behavioral profiling and analysis to gain insights into user activities, potential security threats, and network performance related to encrypted DNS traffic [58].

Kwan et al. [54] developed a method to analyze the browsing history of hosts through the temporal patterns of DNS over TLS (DoT) packet sequences. They identified crucial features across nine categories: query and response lengths, query and response volumes, time intervals, transmission times, DNS packet sequences, and more. By optimizing their models, they achieved good performance with low false negative and false favorable rates, particularly in identifying visited websites. Their techniques also proved effective for padded DoT messages, with high actual favorable rates.

Nguyen et al. [59] explored the security challenges posed by DNS over HTTPS (DoH) and propose a solution using semi-supervised learning to detect malicious DoH tunneling. Traditional DNS queries lack privacy and are vulnerable to various attacks, prompting the adoption of DoH, which encrypts DNS traffic using HTTPS. However, this encryption also enables attackers to hide malicious activities through DoH tunneling. The research employs statistical features and semi-supervised learning classifiers to identify such malicious behavior. The semi-supervised approach achieves high accuracy (98%) while requiring only a small portion of labeled data.

Muhlhauser et al. [60] conducted a study on using n-grams of DNS sequences for classification purposes, explicitly focusing on padded DNS over HTTPS (DoH) and DNS over TLS (DoT) traffic. They found that these classifications could only achieve a 72% accuracy rate, making their classification "ineffective." However, the researchers argue that despite this limitation, the essential characteristics of encrypted DNS traffic remain valuable for future endeavors in user profiling for cybersecurity purposes, such as detecting malware-infected hosts.

Varshney et al. [61] demonstrated their ability to capture DNS over HTTPS (DoH) lookups before encryption by passively monitoring Random Access Memory (RAM) usage on client devices. While DNS encryption aims to safeguard data privacy during transit, it's crucial to understand that organizations and users should not rely on it to thwart such sophisticated attacks in scenarios where a user's device is infected or compromised.

Table 4 compares different research studies on DoH detection using machine learning techniques. The studies were conducted between 2020 and 2022 and used different datasets and methods [62–66]. The results of the studies indicate that machine learning techniques can effectively detect DoH activities, such as intrusion detection, exfiltration detection, and tunneling attack detection. The results also show high levels of accuracy and F1 scores, ranging from 98% to 100%, depending on the method used.

Table 4: The performance results of several studies on detecting DoH using machine learning techniques

Author	Year	Dataset	Method	Result
[6]	2020	DOHBRW-2020	Supervised ML	DoH exfiltration detection with an accuracy of 100%
[53]	2020	DOHBRW-2020	Supervised ML	DoH intrusion detection with the accuracy of 100%
[62]	2020	DOHBRW-2020	Supervised ML	DoH detector with an F1 score of 0.99. DoH exfiltration detector with an F1 score of 0.99
[63]	2020	DOHBRW-2020	Supervised ML	DoH intrusion detector with an F1 score of 0.99. DoH browser identification with an accuracy of 99%
[64]	2021	Custom	Autoencoder	DoH exfiltration detection with an accuracy of 98%
[65]	2021	DOHBRW-2020	Semi-supervised	DoH intrusion detection with an accuracy of 99%
[66]	2022	Custom	Semi-supervised	DoH tunnelling attack detection with an accuracy of 99.4%

5 Research Challenges and Future Studies

DoH [67] is a relatively new technology, and as such, there are still research challenges and future studies that need to be addressed to improve its adoption and effectiveness. We identified several research challenges that must be addressed to promote the adoption and effectiveness of DoH, including performance, security, compatibility, standardization, privacy, and user awareness. We can help realize the full potential of this emerging technology by working to overcome these challenges. Some possible areas of future research challenges include.

5.1 Preventing Malicious Use of DNS over HTTPS (DoH)

DoH communication can be used for malicious purposes such as command and control (C2) communication, data exfiltration, and malware distribution [68]. While previous research has primarily focused on detecting data exfiltration via DoH, other malicious uses, such as C2 communication, have gone undetected. The mechanism malware uses to communicate with its command and control server is called command-and-control (C2) communication [69]. Malware can use DoH to create a secure and encrypted channel for C2 communication, making it difficult for network administrators to detect and prevent such communication. As a result, it is critical to develop new techniques for detecting and preventing various malicious uses of DoH, such as C2 communication. Future research can focus on developing new techniques to detect and prevent various malicious uses of DoH. One approach could be to use machine learning techniques to detect and analyze traffic patterns that indicate malicious activity. Another option is to employ behavior-based analysis techniques to identify the specific characteristics of malicious DoH traffic [70]. The difficulty in developing techniques to detect and prevent malicious DoH uses is ensuring that they effectively identify and block malicious traffic while not interfering with legitimate traffic. Furthermore, the techniques should be able to adapt to changing patterns of malicious DoH traffic and detect new types of malicious activity. Developing effective techniques to detect and prevent malicious DoH uses is critical for ensuring network security and protecting against cyber threats [71].

5.2 Recognition Challenges in DNS over TLS (DoT) Services

Recognition challenges in the context of DNS over TLS (DoT) services refer to the issues associated with the awareness and acknowledgment of the dedicated port TCP/853 within the security community and network infrastructure. This aspect is crucial to DoT's successful implementation, acceptance, and interoperability. One of the primary challenges is the limited awareness of TCP/853 as the designated port for DoT within the security community. Security professionals, network administrators, and other stakeholders may not be fully informed about the importance of this port for secure DNS resolution. The lack of TCP/853 recognition raises concerns about potential firewall blocks. Firewalls typically rely on well-known ports to make decisions about allowing or blocking network traffic. If TCP/853 is not widely recognized, it may lead to unintentional blocks, hindering the effective deployment of DoT [47].

Recognition challenges have broader implications for the widespread acceptance of DoT. For any technology to be adopted on a large scale, it must seamlessly integrate into existing network practices. If the designated port is not uniformly acknowledged, it challenges the smooth acceptance of DoT as a secure DNS resolution method. The lack of standardized recognition for TCP/853 introduces potential interoperability issues. Different systems, DNS resolver services, and client applications may face challenges communicating effectively via DoT if the port is not consistently recognized.

To mitigate these recognition challenges, several strategies can be employed. Educational initiatives such as workshops, training sessions, and informational resources targeted at the security community can enhance awareness about the significance of TCP/853 for DoT. Collaboration between proponents of DoT and the security community is essential, with open channels for information sharing and collaborative efforts helping to bridge the awareness gap. Additionally, advocacy for the standardization of TCP/853 within relevant industry bodies and standards organizations is crucial. Efforts should be directed towards establishing clear guidelines and best practices for using this port in DoT implementations.

Recognition challenges pose a significant hurdle in effectively deploying DNS over TLS services. Addressing these challenges through educational initiatives, collaboration, and standardization advocacy is essential for realizing the full potential of DoT as a secure and widely accepted DNS resolution method.

5.3 Understanding the Impact of DoH on Network Security

The use of DoH can significantly impact network security, and more research is needed to understand these effects [72]. The following are some of the potential effects of DoH on network security:

1. Improved end-user privacy and security: DoH encrypts DNS traffic, making it more difficult for third parties to intercept or manipulate DNS queries and responses. End users may benefit from increased privacy and security due to this.

2. Difficulties for network security professionals: Because they may not be able to see the domain names being accessed, DoH can make it more difficult for network security professionals to analyze network traffic for threat detection and analysis.
3. Increased use of encrypted malware communication: As DoH adoption grows, malware may use encrypted DNS queries to avoid detection and communicate with command and control servers.
4. Difficulty in implementing DNS-based security measures: Many organizations rely on DNS-based security measures, such as firewalls and content filtering, to protect their networks. Adoption of DoH may make the effective implementation of these measures more difficult.

To address these consequences, it is critical to understand how DoH can be used securely and effectively in the context of network security. This includes the development of new privacy-preserving techniques, such as traffic analysis and privacy-preserving proxies, to allow the analysis of DoH traffic without jeopardizing user privacy [41].

5.4 Blocking or Filtering DNS over HTTPS

Current DoH connection blocking/filtering methods are limited and easily circumvented by malware. Malware, for example, can use obscure IP addresses or the same TCP port number as legitimate HTTPS traffic, making differentiation difficult. As a result, blocking or filtering DoH connections based on IP addresses and ports is not an option [73]. Future research can concentrate on developing more robust techniques to effectively identify and block/filter DoH connections while not interfering with legitimate HTTPS traffic. One approach would be to use machine learning-based techniques to analyze traffic patterns and identify abnormal behavior that could indicate DoH use. Another approach would be to use behavioral analysis methods to identify the unique features of DoH traffic that differentiate it from legitimate HTTPS traffic. The difficulty in creating effective DoH blocking/filtering techniques is ensuring they are efficient in identifying and blocking/filtering DoH traffic without obstructing legitimate HTTPS traffic. The methods must also be scalable and flexible enough to accommodate DoH providers' shifting use of IP addresses and ports [3,34].

5.5 DNS Hijacking

DNS spoofing is a malicious technique where attackers provide false or misleading DNS (Domain Name System) responses to redirect users to fraudulent websites. The goal is to deceive users into believing they are accessing a legitimate site when, in fact, they are interacting with a fraudulent one. This deceptive practice involves various tactics, including cache poisoning, man-in-the-middle (MitM) attacks, DNS record tampering, and DNS tunneling. Attackers exploit vulnerable caches, inject false DNS information, intercept DNS queries, and establish covert communication channels through DNS queries and responses. The potential ramifications of DNS spoofing include phishing attacks, malware distribution, and identity theft. Countermeasures against DNS spoofing involve the implementation of DNS Security Extensions (DNSSEC) to ensure data integrity and authentication, the adoption of encrypted DNS protocols (DoH and DoT) to safeguard against eavesdropping and manipulation, regular monitoring, intrusion detection, access control policies, and network segmentation to contain the impact. DNS spoofing remains a persistent and evolving threat, demanding a multifaceted approach for effective mitigation and maintaining a secure digital landscape [74].

5.6 DNS Spoofing

DNS spoofing is a deceptive technique cyber attackers use to mislead users into accessing fraudulent websites while appearing legitimate. This involves manipulating DNS responses and redirecting users to malicious sites that mimic trusted platforms. The deceptive practices of DNS spoofing encompass various methods. In cache poisoning, attackers exploit vulnerable caches by injecting false DNS information and distributing misleading data to users. Users, relying on compromised caches, unknowingly access manipulated IP addresses associated with malicious sites. In Man-in-the-Middle (MitM) attacks, spoofers position themselves between users and DNS servers, intercepting and altering DNS queries. Through real-time manipulation, attackers redirect users to fraudulent sites while maintaining the appearance of normalcy. DNS record tampering involves forgers crafting false DNS responses and introducing incorrect IP addresses for legitimate domain names, leading to the targeted redirection of users attempting to access a specific domain. Additionally, DNS tunneling allows attackers to establish covert communication channels using DNS queries and responses, enabling unauthorized data transfer while circumventing traditional security measures [75].

The potential ramifications of DNS spoofing are diverse. In phishing attacks, spoofed DNS responses mislead users to phishing sites that mimic legitimate platforms. Attackers exploit user trust to harvest sensitive information. Malware distribution is facilitated through DNS spoofing, redirecting users to malicious servers. This can result in users unknowingly downloading and installing malware, compromising the security of their devices. Identity theft is another consequence, as spoofed websites trick users into entering login credentials, potentially leading to unauthorized access to sensitive accounts.

Countermeasures against DNS spoofing include implementing DNS Security Extensions (DNSSEC) to ensure data integrity by signing DNS responses and preventing unauthorized alterations. Validating DNS responses with cryptographic signatures enhances data authentication. Adopting encrypted DNS protocols such as DNS over HTTPS (DoH) and DNS over TLS (DoT) safeguards against eavesdropping and manipulation. Encryption adds a layer of protection, preventing attackers from intercepting and altering DNS traffic. Regular monitoring and intrusion detection are crucial in identifying unusual patterns and signaling potential spoofing attempts. Intrusion detection systems raise alerts when abnormal DNS activities are detected, enabling a swift response. Isolating sensitive network segments helps contain the impact of DNS spoofing, limiting its reach within the infrastructure.

DNS spoofing remains a persistent and evolving threat, necessitating a multi-faceted approach for effective mitigation. Organizations and individuals can fortify their defenses by understanding attacker techniques, recognizing potential risks, and implementing robust countermeasures, contributing to a more secure digital landscape.

5.7 Ensuring the Security of DoH

DoH is vulnerable to various attacks [76] that can compromise its security. DNS spoofing [77] is one such attack where an attacker intercepts and alters the DNS query or response, leading to incorrect IP addresses and thus redirecting the user to a malicious website. Man-in-the-Middle (MITM) attacks occur when an attacker intercepts a user's device and a DNS resolver, allowing them to eavesdrop on the conversation, modify the DNS query or response, and redirect the user to a malicious website.

This is possible because DNS queries and responses are typically transmitted in plain text, making them vulnerable to interception and modification. Secure encryption protocols such as Transport Layer Security (TLS) [78] can encrypt the communication between the user's device and the DNS resolver to prevent MITM attacks. This prevents the attacker from intercepting and modifying the communication. Additionally, verifying the identity of the DNS resolver using techniques such as certificate pinning can ensure that the user is communicating with the intended resolver and not a malicious server. DNS hijacking is another type of attack where an attacker redirects a user to a malicious website by altering the DNS settings of the user's device or network.

To mitigate these types of DoH-based attacks, future research should focus on developing practical techniques. For example, one approach is to use cryptographic mechanisms such as digital signatures to authenticate DNS responses and prevent spoofing attacks.

Another approach is to use certificate pinning, where a device or application checks the authenticity of the certificate presented by the server before establishing a connection. Domain Name System Security Extensions (DNSSEC) can provide a secure DNS infrastructure by digitally signing DNS records and allowing the client to verify their authenticity. While significant research is needed to understand the impact of DNS over HTTPS (DoH) on network security, it is also essential to highlight the importance of practical engineering efforts and the broader adoption of emerging techniques. Theoretical insights gained from research must be complemented by real-world implementation and practical experience. Laboratory research alone cannot capture the full spectrum of DoH's impact on network security. Practical deployment and widespread use of DoH in diverse environments are crucial. This approach provides valuable insights into real-world challenges and opportunities, facilitating the development of robust security solutions that are effective in operational settings. Collaboration between academic researchers and industry professionals is vital. By working together, they can ensure that theoretical findings are effectively translated into practical applications, leading to the successful integration of DoH into network security practices.

While ongoing research is crucial, it must go hand in hand with practical engineering efforts and the broader adoption of emerging techniques. This integrated approach is essential for fully understanding and leveraging the potential of DoH to enhance network security [51,79]. Table 5 highlights the key research challenges and future studies required for the successful integration and deployment of DoH technology. These research challenges and future studies are critical to the adoption and effectiveness of DoH and to ensuring network security and protection against cyber threats. On the other hand, Table 6 highlights the critical research challenges and future studies required for the successful integration and deployment of DoH technology.

Table 5: Advantages and disadvantages of different approaches for detecting DoH traffic and attacks

Approach	Advantages	Disadvantages
Signature	Based on fast and simple	May miss new or unknown DoH traffic
Behaviour-based	Can detect unknown DoH traffic	More complex and slower than signature-based methods
Machine learning based	Can detect unknown and new DoH traffic and attacks	Requires a large and diverse dataset for training and may be susceptible to adversarial attacks

Table 6: The key research challenges and future studies required for successful integration and deployment of DoH technology

Research challenges	Description
Compatibility	Ensure compatibility of DoH with existing DNS infrastructure
Standardization	Standardize the implementation of DoH to ensure interoperability and compatibility between different DoH providers and clients
Privacy	Investigate and improve the privacy of DoH to protect user data and prevent third-party tracking and surveillance
User awareness	Educate end users about DoH, its benefits, and potential risks to increase adoption and awareness of the technology
Impact on network security	Investigate the impact of DoH on network security, develop privacy-preserving techniques, and ensure the security of encrypted traffic
Blocking or filtering	DoH Develop more robust techniques to effectively identify and block/filter DoH connections without interfering with legitimate HTTPS traffic
Ensuring DoH security	Develop effective techniques to mitigate DoH-based attacks, use secure encryption protocols, and verify the identity of the DNS resolver

6 Conclusions

We provide a comprehensive review of the impact of DNS over HTTPS (DoH) on cybersecurity, encompassing an analysis of its limitations, challenges, and instances of abuse on the internet. We highlight various techniques and methodologies for effectively detecting DoH tunneling activities, which are essential for maintaining network security in the DoH environment. Furthermore, we identify and discuss key research challenges crucial for future security studies in DoH. These challenges emphasize compatibility with existing DNS infrastructure, standardization, privacy concerns, user awareness, and the impact on network security. Additionally, we raise awareness regarding potential security vulnerabilities associated with DoH. We aim to promote a better understanding of the risks and challenges posed by this technology, emphasizing the need to develop and implement effective security solutions to mitigate these risks and ensure user privacy and data protection.

Acknowledgement: The authors would like to express their gratitude for the valuable feedback and suggestions provided by all the anonymous reviewers and the editorial team.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a large group Research Project under Grant Number RGP.2/373/45.

Author Contributions: Conceptualization: Muhammad Dawood; validation: Shanshan Tu, Chuangbai Xiao; formal analysis: Muhammad Haris, Hisham Alasmary; writing—original draft: Muhammad Dawood, Muhammad Waqas; writing—review & editing: Muhammad Waqas, Sadaqat Ur Rehman;

supervision: Shanshan Tu, Muhammad Waqas, Chuangbai Xiao. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] E. Rescorla, H. Tschofenig, and N. Modadugu, "RFC 9147: The datagram transport layer security (DTLS) protocol version 1.3," *Internet Eng. Task Force*, vol. 1, no. 1, 2022.

[2] Y. Wang, A. Zhou, S. Liao, R. Zheng, R. Hu and L. Zhang, "A comprehensive survey on DNS tunnel detection," *Comput. Netw.*, vol. 197, 2021, Art. no. 108322.

[3] K. Hynek, D. Vekshin, J. Luxemburk, T. Cejka, and A. Wasicek, "Summary of DNS over HTTPS abuse," *IEEE Access*, vol. 10, pp. 54668–54680, 2022.

[4] DNSCrypt, "dnscrypt-proxy," *GitHub*. DNSCrypt GitHub Repository. Mar. 25, 2023.

[5] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on DNS encryption: Current development, malware misuse, and inference techniques," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–28, 2022.

[6] A. S. Jahromi and A. Abdou, "Comparative analysis of DoT and HTTPS certificate ecosystems," in *Workshop Meas., Attacks, Defenses Web (MADWeb) 2021*, Feb. 25, 2021.

[7] F. J. Nijeboer, "Detection of HTTPS encrypted DNS traffic," Bachelor's thesis, Dept. of Electrical Engineering, Mathematics and Computer Science, Univ. of Twente, Enschede, Netherlands, 2020.

[8] O. M. Bonastre and A. Vea, "Origins of the domain name system," *IEEE Ann. Hist. Comput.*, vol. 41, no. 2, pp. 48–60, 2019. doi: 10.1109/MAHC.2019.2913116.

[9] C. Deccio and J. Davis, "DNS privacy in practice and preparation," in *Proc. 15th Int. Conf. Emerg. Netw. Exp. Technol.*, Orlando Florida, Dec. 9–12, 2019, pp. 138–143.

[10] T. Böttger *et al.*, "An empirical study of the cost of DNS-over-HTTPS," in *Proc. Internet Meas. Conf.*, Amsterdam, Netherlands, Oct. 21–23, 2019, pp. 15–21.

[11] IETF, "DNS queries over HTTPS (DoH)-request for comments 8484," 2018. Accessed: Mar. 26, 2023. [Online]. Available: https://tools.ietf.org/html/rfc8484

[12] Cloudflare, "Connecting apps in cloudflare one," Accessed: Mar. 23, 2023. [Online]. Available: https://developers.cloudflare.com/cloudflare-one/connections/connect-apps

[13] Facebook, "doh-proxy," Accessed: Mar. 25, 2023. [Online]. Available: https://github.com/facebookexperimental/doh-proxy

[14] M. Sammour, B. Hussin, M. F. Othman, M. Doheir, B. AlShaikhdeeb and M. S. Talib, "DNS tunneling: A review on features," *Int. J. Eng. Technol.*, vol. 7, no. 3.20, pp. 1–5, 2018.

[15] M. Al-Fawa'reh, Z. Ashi, and M. T. Jafar, "Detecting malicious DNS queries over encrypted tunnels using statistical analysis and bi-directional recurrent neural networks," *Karbala Int. J. Mod. Sci.*, vol. 7, no. 4, 2021. doi: 10.33640/2405-609X.3155.

[16] R. Houser, Z. Li, C. Cotton, and H. Wang, "An investigation on information leakage of DNS over TLS," in *Proc. ACM CoNEXT*, Orlando, Florida, 2019, pp. 123–137.

[17] M. Waqas, S. Tu, Z. Halim, S. Rehman, G. Abbas and H. Z. Abbas, "The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges," *Artif. Intell. Rev.*, vol. 55, pp. 5215–5261, 2022. doi: 10.1007/s10462-022-10143-2.

[18] D. Herrmann, C. Banse, and H. Federrath, "Behavior-based tracking: Exploiting characteristic patterns in DNS traffic," *Comput. Secur.*, vol. 39, pp. 17–33, 2013. doi: 10.1016/j.cose.2013.03.012.

[19] M. Konopa, J. Fesl, J. Jelínek, M. Feslová, J. Cehák, and J. Janeček, “Using machine learning for DNS over HTTPS detection,” in *19th Eur. Conf. Cyber Warf.*, 2020, p. 205.

[20] M. Aiello, A. Merlo, and G. Papaleo, “Performance assessment and analysis of DNS tunneling tools,” *Logic J. IGPL*, vol. 21, no. 4, pp. 592–602, 2013. doi: 10.1093/jigpal/jzs029.

[21] A. Merlo, G. Papaleo, S. Veneziano, and M. Aiello, “A comparative performance evaluation of DNS tunneling tools,” in *Comput. Intell. Secur. Inform. Syst., CISIS 2011*, Torremolinos-Málaga, Spain, Jun. 8–10, 2011, pp. 84–91.

[22] J. Zhang, L. Yang, S. Yu, and J. Ma, “A DNS tunneling detection method based on deep learning models to prevent data exfiltration,” in *Netw. Syst. Secur.: 13th Int. Conf., NSS 2019*, Sapporo, Japan, Dec. 15–18, 2019, pp. 520–535.

[23] L. F. G. Casanova and P. C. Lin, “Malicious network traffic detection for DNS over HTTPS using machine learning algorithms,” *APSIPA Trans. Signal Inf. Process*, vol. 12, no. 2, 2023.

[24] NextDNS, “The new firewall for the modern Internet,” Accessed: Mar. 20, 2024. [Online]. Available: https://nextdns.io/

[25] P. Wu, “Understanding DNS encryption,” *Cloudflare Blog*. Accessed: Jun. 28, 2023. [Online]. Available: https://blog.cloudflare.com/dns-encryption-explained/

[26] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, “Encrypted DNS→ privacy? A traffic analysis perspective,” 2019, *arXiv:1906.09682*.

[27] Y. Zeng *et al.*, “Finding disposable domain names: A linguistics-based stacking approach,” *Comput. Netw.*, vol. 184, Jan. 2021, Art. no. 107642. doi: 10.1016/j.comnet.2020.107642.

[28] M. Kosek, T. V. Doan, M. Granderath, and V. Bajpai, “One to rule them all? A first look at DNS over QUIC,” in *Proc. Int. Conf. Passive Active Netw. Meas.*, Switzerland, Cham, 2022, pp. 537–551.

[29] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, “Comparing the effects of domain name system, DNS over transport layer security, and DNS over HTTPS on web performance,” in *Proc. Web Conf.*, 2020, pp. 562–572.

[30] K. Borgolte *et al.*, “How DNS over HTTPS is reshaping privacy, performance, and policy in the internet ecosystem,” in *TPRC47, 47th Res. Conf. Commun., Inform. Internet Policy*, WA, Washington, USA, American University’s Washington College of Law (WCL), 2019, pp. 1–13.

[31] R. Houser, S. Hao, Z. Li, D. Liu, C. Cotton and H. Wang, “A comprehensive measurement-based investigation of DNS hijacking,” in *40th Int. Symp.Reliab. Distrib. Syst. (SRDS)*, Chicago, IL, USA, Sep. 2021, pp. 210–221.

[32] S. Rivera, V. K. Gurbani, S. Lagraa, A. K. Iannillo, and R. State, “Leveraging eBPF to preserve user privacy for DNS, DoT, and DoH queries,” in *Proc. 15th Int. Conf. Availability, Reliab. Secur.*, Ireland, Aug. 25–28, 2020, pp. 1–10.

[33] C. Lu *et al.*, “An end-to-end, large-scale measurement of DNS-over-encryption: How far have we come?,” in *Proc. Internet Meas. Conf.*, Amsterdam, Netherlands, Oct. 21–23, 2019, pp. 22–35.

[34] Q. Huang, D. Chang, and Z. Li, “A comprehensive study of DNS-over-HTTPS downgrade attack,” in *Proc. 10th USENIX Workshop Free Open Commun. Internet (FOCI 20)*, 2020, pp. 1–7.

[35] A. Nisenoff, N. Feamster, M. A. Hoofnagle, and S. Zink, “User expectations and understanding of encrypted DNS settings,” in *Proc. NDSS DNS Priv. Workshop*, 2021, pp. 1–8.

[36] M. Vale and A. Dupuy, “Google public DNS over HTTPS (DoH) supports RFC 8484 standard,” google security blog. 2019. Accessed: Jul. 21, 2023. [Online]. Available: https://security.googleblog.com/2019/06/google-public-dns-over-https-doh.html

[37] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, “Large scale measurement on the adoption of encrypted DNS,” 2021, *arXiv:2107.04436*.

[38] C. Hesselman *et al.*, “The DNS in IoT: Opportunities, risks, and challenges,” *IEEE Internet Comput.*, vol. 24, no. 4, pp. 23–32, 2020. doi: 10.1109/MIC.2020.3005388.

[39] S. Tu, M. Waqas, A. Badshah, M. Yin, and G. Abbas, “Network intrusion detection system (NIDS) based on pseudo-Siamese stacked autoencoders in fog computing,” *IEEE Trans. Serv.. Comput.*, vol. 16, no. 6, pp. 4317–4327, 2023. doi: 10.1109/TSC.2023.3319953.

[40] C. López Romera, "DNS over HTTPS traffic analysis and detection," M.S. thesis, Dept. Informatics, Universitat Oberta de Catalunya (UOC), Spain, 2020.

[41] C. Patsakis, F. Casino, and V. Katos, "Encrypted and covert DNS queries for botnets: Challenges and countermeasures," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101614. doi: 10.1016/j.cose.2019.101614.

[42] B. Sun, Q. Y. Wen, and X. Y. Liang, "A DNS-based anti-phishing approach," in *2010 Second Int. Conf. Netw. Secur., Wireless Commun. Trust. Comput.*, IEEE, 2010, vol. 2, pp. 262–265. doi: 10.1109/NSWCTC.2010.196.

[43] K. Hynek and T. Cejka, "Privacy illusion: Beware of unpadded DoH," in *Proc. 2020 11th IEEE Annu. Inform. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Vancouver, BC, Canada, Nov. 4–7, 2020, pp. 621–628.

[44] N. U. Aijaz, M. Misbahuddin, and S. Raziuddin, "Survey on DNS-specific security issues and solution approaches," in *Data Science and Security*, Springer Singapore: Singapore, 2021, pp. 79–89.

[45] M. N. Banu and S. M. Banu, "A comprehensive study of phishing attacks," *Int. J. Comput. Sci. Inform. Technol.*, vol. 4, no. 6, pp. 783–786, 2013.

[46] E. Heftrig, H. Shulman, and M. Waidner, "Poster: Off-path DNSSEC downgrade attacks," in *Proc. ACM SIGCOMM, 2023 Conf.*, New York, NY, USA, Sep. 10, 2023, pp. 1120–1122.

[47] A. M. Kosh *et al.*, "An insight into encrypted DNS protocol: DNS over TLS," in *4th Int. Conf. Recent Develop. Control, Autom., Power Eng. (RDCAPE)*, Noida, India, Oct. 7–8, 2021, pp. 379–383.

[48] W. B. de Vries, Q. Scheitle, M. Müller, W. Toorop, R. Dolmans and R. Van Rijswijk-Deij, "A first look at QNAME minimization in the domain name system," in *20th Int. Conf., PAM 2019*, Puerto Varas, Chile, Mar. 27–29, 2019, pp. 147–160.

[49] G. C. M. Moura, S. Castro, W. Hardaker, M. Wullink, and C. Hesselman, "Clouding up the internet: How centralized is DNS traffic becoming?," in *Proc. ACM Internet Meas. Conf.*, Oct. 27–29, 2020, pp. 42–49.

[50] A. Alabduljabbar, R. Ma, S. Choi, R. Jang, S. Chen and D. Mohaisen, "Understanding the security of free content websites by analyzing their SSL certificates: A comparative study," in *Proc. 1st Workshop Cybersecur. Soc. Sci.*, Nagasaki, Japan, May 30, 2022, pp. 19–25.

[51] R. Mitsuhashi, A. Satoh, Y. Jin, K. Iida, T. Shinagawa, and Y. Takai, "Identifying malicious DNS tunnel tools from DoH traffic using hierarchical machine learning classification," in *24th Int. Conf. Inform. Secur. (ISC 2021)*, Nov. 10–12, 2021, pp. 238–225.

[52] D. Vekshin, K. Hynek, and T. Cejka, "DoH insight: Detecting DNS over HTTPS by machine learning," in *Proc. 15th Int. Conf. Availability, Reliab. Secur.*, Aug. 25–28, 2020, pp. 1–8.

[53] S. Singh, S. K. Kumar, and P. K. Roy, "Detecting malicious DNS over HTTPS traffic using machine learning," in *Proc. 2020 Int. Conf. Innov. Intell. Inform., Comput., Technol. (3ICT)*, Sakheer, Bahrain, IEEE, Dec. 20–21, 2020, pp. 1–6.

[54] P. Kwan, S. Janiszewski, S. Qiu, C. Wang, and C. Bocovich, "Exploring simple detection techniques for DNS-over-HTTPS tunnels," in *Proc. ACM SIGCOMM, 2021 Workshop Free Open Commun. Internet*, USA, Aug. 27, 2021, pp. 37–42.

[55] A. R. Alzighaibi, "Detection of DoH traffic tunnels using deep learning for encrypted traffic classification," *Computers*, vol. 12, no. 3, 2023, Art. no. 47. doi: 10.3390/computers12030047.

[56] M. MontazeriShatoori, L. Davidson, G. Kaur, and A. H. Lashkari, "Detection of DoH tunnels using time-series classification of encrypted traffic," in *Int. Conf. Dependable, Autonom. Secure Comput.*, Calgary, AB, Canada, Aug. 17–22, 2020, pp. 63–70.

[57] W. Kumari *et al.*, "SAC109—The implications of DNS over HTTPS and DNS over TLS," in *ICANN Secur. Stability Advis. Committee (SSAC) Rep. Advis.*, 2020.

[58] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster, "Can encrypted DNS be fast?," in *Proc. Passive Active Meas.: 22nd Int. Conf., PAM 2021*, Mar. 29–Apr. 1, 2021, pp. 444–459.

[59] A. T. Nguyen and M. Park, "Detection of DoH tunneling using semi-supervised learning method," in *Int. Conf. Inf. Netw. (ICOIN)*, Jeju-Si, Republic of Korea, Jan. 12–15, 2022, pp. 450–453.

[60] M. Mühlhauser, H. Pridöhl, and D. Herrmann, "How private is Android's private DNS setting? Identifying apps by encrypted DNS traffic," in *Proc. 16th Int. Conf. Availability, Reliab. Secur. (ARES)*, Vienna, Austria, 2021.

[61] G. Varshney, P. Iyer, P. Atrey, and M. Misra, "Evading DoH via live memory forensics for phishing detection and content filtering," in *Proc. 13th Int. Conf. COMmun. Syst. NETw. (COMSNETS)*, 2021.

[62] M. MontazeriShatoori, "An anomaly detection framework for DNS-over-HTTPS (DoH) tunnel using time-series analysis," Ph.D. thesis, University of New Brunswick, Canada, 2020.

[63] Y. M. Banadaki and S. Robert, "Detecting malicious DNS over HTTPS traffic in domain name system using machine learning classifiers," *J. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 46–55, 2020. doi: 10.12691/jcsa-8-2-2.

[64] J. Wu, Y. Zhu, B. Li, Q. Liu, and B. Fang, "Peek inside the encrypted world: Autoencoder-based detection of DoH resolvers," in *20th Int. Conf. Trust, Secur. Priv. Comput. Commun. (TrustCom)*, 2021, pp. 783–790.

[65] L. F. G. Casanova and P. C. Lin, "Generalized classification of DNS over HTTPS traffic with deep learning," in *Proc. 2021 Asia-Pacific Signal Inform. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Tokyo, Japan, Dec. 14–17, 2021, pp. 1903–1907.

[66] T. A. Nguyen and M. Park, "DoH tunneling detection system for enterprise network using deep learning technique," *Appl. Sci.*, vol. 12, no. 5, 2022, Art. no. 2416. doi: 10.3390/app12052416.

[67] P. Mockapetris, "Domain names-implementation and specification," RFC 1035, Internet Engineering Task Force, Nov. 1987. Accessed: Jul. 21, 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1035

[68] R. Guo, J. Du, X. Chen, and S. Shu, "A DNS-based data exfiltration traffic detection method for unknown samples," in *7th IEEE Int. Conf. Data Sci. Cyberspace (DSC)*, Guilin, China, 2022, pp. 191–198.

[69] K. Xu, P. Butler, S. Saha, and D. Yao, "DNS for massive-scale command and control," *IEEE Trans. Dependable Secur. Comput.*, vol. 10, no. 3, pp. 143–153, 2013. doi: 10.1109/TDSC.2013.10.

[70] K. Jerabek, K. Hynek, and O. Rysavy, "Comparative analysis of DNS over HTTPS detectors," *Comput. Netw.*, vol. 247, 2024, Art. no. 110452. doi: 10.1016/j.comnet.2024.110452.

[71] R. Alenezi and S. A. Ludwig, "Classifying DNS tunneling tools for malicious DoH traffic," in *IEEE Symp. Series Comput. Intell. (SSCI)*, Orlando, FL, USA, 2021, pp. 1–9.

[72] L. Jin, S. Hao, H. Wang, and C. Cotton, "Understanding the impact of encrypted domain name system on internet censorship," in *Proc. Web Conf.*, Ljubljana, Slovenia, 2021, pp. 484–495.

[73] A. Aggarwal and M. Kumar, "An ensemble framework for detection of DNS-over-HTTPS (DoH) traffic," *Multimed. Tools Appl.*, vol. 83, no. 11, pp. 32945–32972, 2024. doi: 10.1007/s11042-023-16956-9.

[74] M. Fejrskov, J. M. Pedersen, and E. Vasilomanolakis, "Detecting DNS hijacking by using NetFlow data," in *Proc. 2022 IEEE Conf. Commun. Netw. Secur. (CNS)*, Austin, TX, USA, 2022, pp. 273–280.

[75] C. Deccio, A. Hilton, M. Briggs, T. Avery, and R. Richardson, "Behind closed doors: A network tale of spoofing, intrusion, and false DNS security," in *Proc. ACM Internet Meas. Conf. (IMC)*, USA, Oct. 27–29, 2020, pp. 65–77.

[76] K. Jerabek, K. Hynek, O. Rysavy, and I. Burgetova, "DNS over HTTPS detection using standard flow telemetry," *IEEE Access*, vol. 11, pp. 50000–50012, 2023. doi: 10.1109/ACCESS.2023.3275744.

[77] A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev, "Detection and prevention of DNS spoofing attacks," in *Proc. Siberian Symp. Data Sci. Eng. (SSDSE)*, Novosibirsk, Russia, Apr. 12–13, 2017, pp. 84–87.

[78] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)," RFC 7858, RFC Editor. 2016. Accessed: Jun. 28, 2023. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7858.html

[79] T. H. Kim and D. Reeves, "A survey of domain name system vulnerabilities and attacks," *J. Surveill. Securit. Safety*, vol. 1, no. 1, pp. 34–60, 2020. doi: 10.20517/jsss.2020.14.