The Era of Secure DNS: An Overview on Security and Best Practices

Asad Ali Akbar Shirazi
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
asadshirazipro@gmail.com

Zain ul Abiden Akhtar
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
engr.zain@iub.edu.pk

Mubashir Shaheen
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
mubashershaheen8@gmail.com

Hafiz Muhammad Hamza Sohail
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
mrhamzaoffical1@gmail.com

***Abstract*—The internet infrastructure functionally utilizes the Domain Name System (DNS) which takes domain names through its translation process as a bridge to IP addresses to create successful online connections. The basic infrastructure of the DNS system exposes security risks because weak protection measures allow attackers to perform DNS spoofing, cache poisoning, DDoS attacks, hijacking, tunneling, and advanced persistent threats attacks and steal data. This paper examines mitigation methods and techniques such as DNSSEC,DoH threat intelligence automation, and secure resolvers like Quad9 and Cloudflare and their implementation for DNS security matters through an analysis of key DNS elements while detailing usual attack methods and the extensive risks of DNS breaches that manifest as noncompliance issues and operational breakdowns.**

***Index Terms*—Cyber security, Domain Name System (DNS), Decentralization, DNS Tunneling, DNS Spoofing, DNS Security (DNSSEC), DDoS, DNS attacks, Network Security**

I. Introduction

The Domain Name System (DNS) that makes accessing the Internet easier by converting readable domain names such as www.akamai.com into computer-friendly IP addresses like 104.101.221.0 that tell web browsers and services how to proceed. Speed, scalability, and reliability were first considered when building DNS while security and privacy were not at the forefront of considerations. Although DNS attacks have come to the fore over thirty years ago, the DNS network, despite upgrading, continues to operate largely in the original framework and it is a critical component in supporting access to services, data, and devices. Although DNSSEC has been deployed more widely in the last few years, attacks on the DNS have intensified in terms of both number and complexity. Such attacks cross boundaries, mutate regularly, adjust to new plans and are capable of bypassing standard information security countermeasures such as firewalls and loss of data prevention [1].

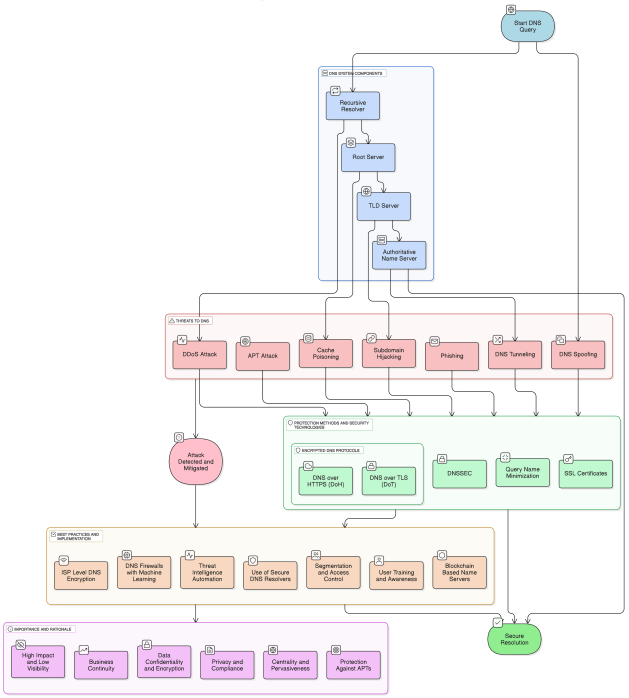

Fig. 1. Taxonomy

A. DNS and its Functions

The Domain Name System (DNS) is the foundational process upon which Internet users and services communicate with each other. Since its establishment, DNS has developed with the introduction of many database indexes to address existing problems, meet new needs. These challenges are growing continuously. Developments in interception of the DNS detection have prompted development to improve the privacy of the DNS queries [2]. As an example, every time one types in “Example.com” in his/her web browser, the server

DOI: https://doi.org/10.67535/tsp.000001.030
Published under the ICACNC 2025 Proceedings

is directed to change the domain name to an IP address like 1.2.3.4 after which the browser and other online activities such as transfers of files are able to work well. The DNS system runs with a hierarchical level of servers around the Internet [3].

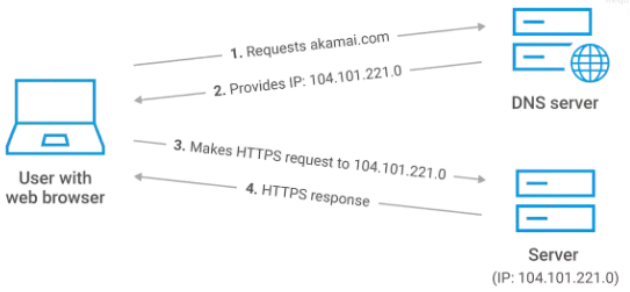

Fig. 2. DNS Query Process

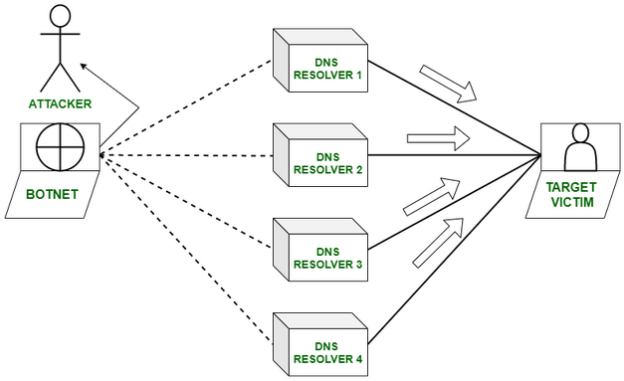

Fig. 3. DNS Amplification Attack

A DNS system contains multiple fundamental elements as:

- **Name servers**: Act as authorities to provide the final IP address for a domain.
- **Root servers**: The resolver reaches TLD (Top Level Domains) servers through the route provided by root servers.The DNS hierarchy has at its top or root the root DNS servers. In the world, there are thirteen (13) root name servers [4].
- **Recursive resolvers**: Following user query reception, the recursive resolvers perform the search operations.
- **TLD servers**: The message moves from TLD servers to authoritative name servers through the TLD servers' network.

B. DNS Threats

Cyber criminals abuse DNS vulnerabilities to conduct rerouting, data theft, or system overload attacks. The primary DNS security risks consist of the following:

DNS Spoofing The DNS spoofing attacks inject deceptive data into the DNS resolver's cache and do so covertly and cunningly redirecting visitors to dangerous domains. These attacks allow the fraudsters to redirect people accessing financial sites to phishing pages attempting to harvest secret login data. The incidence of DNS spoofing attacks has almost doubled in the past seven years, and the use of proxy servers has been found to be the main source of such worldwide events [5].

DDos Attacks On DNS An incident occurred in October 2016 when a program compromised tens of thousands of connected cameras and home devices and used them to conduct synchronized wave of distributed denial-of-service, (DDoS) attacks in a matter of hours. Application of this technique exposed a significant network security loophole in the current Internet configuration. Furthermore, there was a symbolic gesture in the attack, which targeted Dyn, a provider of reputation services like CNBC, Netflix and Twitter [6]. Query-crafting DoS threats exacerbate the effects on the DNS systems of the DoS attacks by increasing the communication and the time, and identifying the detection features can contribute to the protection against them [7].

Cache poisoning DNS is a victim of many challenges including cache poisoning, and so attracts cybercriminals. To increase Internet speed, the DNS servers keep large local copies of the DNS records at regional archives [8].DNS poisoning is one of the most treacherous vectors whereby a culprit introduces harmful entries into the DNS resolution, thus, forcing the clients to be redirected from the genuine to malicious servers [9].

Hijacking of Subdomains The assaults on the domain name system, DNS, have been long-time plagues of the Internet, which must be studied and watched over constantly, so as not to misuse this important structure. Of these attacks, the DNS hijacking has several times confirmed itself as the most severe threat [10]. In 2019, the US Department of Homeland Security sent out a warning regarding DNS infrastructure tampering – in an emergency. This alert being a reaction resulting from a chain of attacks on overseas government related websites which compromised DNS [11].

DNS Tunneling Criminals use malicious botnets that benefit from DNS tunneling to send malicious commands and control signals towards the taken network. Yet, there exist many impediments to detection of DNS tunneling attacks [12].Tunnels used in the domain name system (DNS), created between the controlled host/host and master server (itself masquerading as such authoritative / authoritative domain name server, can be used as secret channel for data communications, that can be malicious [13].

APT Attacks Advanced Persistent Threat (APT) attack is one of the types of malicious, aimed, targeted attack. By cause of applying a variety of advanced and complex techniques and technologies to target the process of attack to acquire confidential and sensitive information [14].

Phishing Attacks Phishing is one of Cyber attack where the user is redirected to bogus websites and compromised to submit his – her sensitive and personal information such as

passwords of accounts, bank details, atm pin-card details , rouge DNS ervers with sniffing methods,.etc. Therefore, the protection of sensitive data against malwares/web phishing is challenging and it requires awareness of users [15].

II. Methodology

The Domain Name System (DNS) is the backbone of the Internet, translating readable domain names into machine-readable IP addresses. Anycast routing, especially with Cloudflare WARP, increases DNS resilience against DDoS attacks and keeps the service available with an average response time of 172.44 ms before and 117.66 ms after each attack [16].The challenges, in terms of DNS records' consistency and tracking over time, associated with their management can have operational impacts, especially in the cybersecurity aspect [17].

A. DNS Protection Methods

Several DNS protection methods have been developed and implemented:

- **DNSSEC: Domain Name System Security Extensions**By including cryptographic signatures in DNS records, DNSSEC allows DNS clients to validate whether or not the DNS data they receive are authentic. Towards this end, DNSSEC introduces new signatures, namely, RRSIG, DNSKEY and DS, into the DNS scheme. Responding to a DNSSEC supported query, the DNS resolver can request the DNS server to provide the recorded signatures together with a matching public key [18].The agility of DNSSEC enables the deployment of new ciphers, but at the same time, can put its users at risk, as 45 percent of the web clients will become vulnerable to attacks [19].
- **Encrypted DNS Protocols (DoH and DoT)**The protocol does HTTPS over HTTP encryption of DNS data and forwards it to TCP port 443. DoH is preferable as it conforms to the present security procedures and is the norm protocol in many web browsers (including HTTPS) [20]. When the connection is used for a single query DoH introduces a lot of latency. Nevertheless, DoH connection is reused for more than one query where the additional time is trivial. Another research carried out by Hounsel et al. reveals that DoH latency and reliability are highly dependent on the chosen resolver [21].This is also confirmed by Jerabek et al who worked on the behavior of DoH resolver and distribution of DoH packets sizes for various used resolvers. Based on their outcomes, some of the DoH resolvers employ long HTTP headers that translate to larger packets, and therefore, a higher overhead [22].
- **Query Name Minimization**: Query name Minimization provides means to build up DoH query privacy. Once the implementation of DoH occurs, DNS queries are encrypted then sent to a remote server over HTTPS. This helps to keep the privacy and undisturbed state of the queries, as they move. However, after the query is received through the remote server, the server will be able to log or explore it, and this condition might expose sensitive user data [23].
- **SSL Certificates**:SSL certificates function as digital files that encrypt-service cryptic keys with information of an organization such as hostnames, server names, domain-names and properties like uniqueness of organization and geographical location. The use of SSL certificates ensures a secured channel between websites and browsers and protect that sensitive user information including log in credentials and financial transaction [24].

B. Importance of DNS Security

The default DNS resolver of an Internet Service Provider (ISP) may not be desirable due to such reasons as censorship, no options for malware filtering and poor quality of service [25] . affecting reputation, operational continuity, financial stability, and regulatory compliance:

1) High Impact and Low Visibility: Today, businesses focus their security checks on HTTP/S, FTP, or SMTP traffic while bypassing DNS traffic analysis. Hackers exploit this unidentified DNS activity zone because DNS creates a blind spot for security systems. DNS tunneling allows cybercriminals to hide their control communications through disguised DNS query traffic.Due to the overdependence on little miners of large DNS servers, the risks of the data leaks and the services interruption in a case if failures and if the digital sovereignty over the DNS hosting in the countries [26].

2) Preventing Disruption in Business: When DNS systems fail, it leads to immediate sales losses among internet merchants, particularly when peak consumer activity occurs. Thre business use DNSGuard is a smart in-network defense paradigm that is able to thwart volumetric and non-volumetric DNS attacks using programmable switches with hardly the nanosecond's worth of latency in highly loaded networks [27]. Also use The load balancing that enhance security; they are proposed to eliminate disruption of business because of IoT DNS flood attacks [28].

3) Data Confidentiality and Encryption: ADNS enforce policy for all names in its domain authority: any TEE running the service must provide a hardware certificate that meets the domain-specific policy before it can register keys and certificates for any name in the domain. ADNS provides protocols for delegation of zones, registration of TEEs and the creation of attestations [29].

4) Data Privacy and Compliance: Domain name system administrators could take more stringent measures to reduce the incidence and consequences of DNS abuse. In 2018, the amount of information available to domain name owners for public purposes was limited in accordance with the provisions of the General Data Protection Regulation [30].

5) Centrality and Pervasiveness: Research has made clear how concentrated the market share and the volume of DNS traffic has been of public DNS services, as seen by the leading CDN providers. Meanwhile little about the extent of

centralisation, that occurs within DNS ecosystem infrastructure, is known [31].The DNS infrastructure is much more concentrated than previously assumed, and 0.45 percent of the name servers are providing authoritative domain resolution service for 48.5 percent of the domain names [32].

6) Protection against Advanced Persistent Threats (APTs): The security community has gotten more concerned about APT attacks on sensor systems. Given the limited security installed in sensors, the APT attack organization can create plans that can support them to infiltrate, attack, evade detection, proliferate and extract data from a target for an extended period. Researchers discovered that surveillance of DNS traffic during the communication control phase helps in detecting APT attacks to a significant extent by conducting an in-depth analysis of APT attacks methodologies and associated countermeasures [33].

Table 1: Summary of DNS Protection Methods

Method	Core Features	Strengths	Limitations
DNSSEC	Cryptographic signatures for data authenticity.	Prevents spoofing, cache poisoning.	31% missing records; 45% clients vulnerable.
DoH/DoT	Encrypts queries via HTTPS/TLS.	Blocks eavesdropping, ISP injection.	DoH latency; resolver-dependent.
Query Name Minimization	Sends minimal query data.	Boosts privacy; less data leakage.	Relies on resolver trust.
SSL Certificates	Encrypts channels; authenticates servers.	Secures data in transit.	No DNS attack protection.
DNS Firewalls with ML	ML blocks malicious domains.	Real-time protection; adaptive.	Needs accurate threat lists.
Threat Intelligence Automation	AI/ML for DNS filtering.	Scalable; detects complex threats.	Risks false positives; complex.
Secure DNS Resolvers	Services with encryption, blocking.	Easy to use; secure.	Centralized; privacy risks.
Segmentation & Access Control	Limits resolver access; RBAC.	Stops malware; secure changes.	Complex setup; strict enforcement.
Blockchain Name Servers	Decentralized namespace.	Less centralized; resilient.	Scalability issues; complex adoption.

Fig. 4. Summary of DNS Protection methods

III. Implementation

A. DNSSEC or DoH at ISPs Level

ISP level should be used by DNS Encryption.Several DNS Encryption proposals were presented in 2016 but no detailed examination on their implementation is made. This research gauged the level of adoption of DoH (DNS over HTTPS), DoT (DNS over TLS) in the last five months of the year 2021 by three different organizations, catering to the world [34].5G also has no DNS security .

- The latency in 5G networks should be 1-4 ms in the RAN, so DNS needs to be optimized to avoid becoming a bottleneck. DNS architectures that are placed in the middle of the network have a hard time responding to the growing demand.
- Because of new features like network slicing, virtualization, and edge computing, the attack surface on 5G networks has grown. Attacks like spoofing, cache poisoning, and DDoS occur more often because of more devices and spread of computing.
- Since IoT and M2M connections are rising, DNS on 5G networks must handle a large number of queries quickly and efficiently.
- When DNS traffic is unencrypted, it allows ISPs to keep an eye on people's browsing records. People can circumvent ISP DNS servers by using encrypted protocols, which ISPs find hard to detect.

By analyzing the DNS resolution process in the 5G network in details, it is found that 5G network lacks the security loophole of checking validity of the DNS query destination IP [35].DNSSEC has deployment problems in the contemporary Internet. Chung et al. discovered that domains supplying DNSSEC had failed to publish all the necessary records for validation in 31 percent of cases and that 39 percent had used either a weak or an insecure key-signing key. They also discovered that 82 percent of the resolvers asked for DNSSEC records while only 12 percent of them tried to validate the DNSSEC records [36].

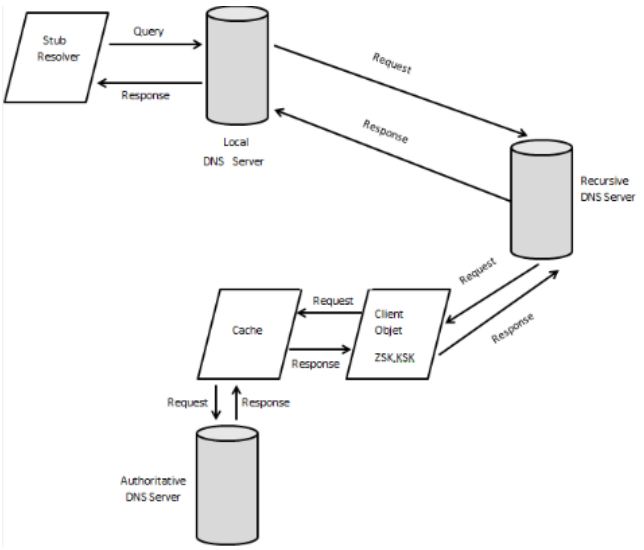

Fig. 5. DNSSEC Workflow

B. DNS Firewalls with ML

The use of ML inside DNS firewalls so that it can detect malicious domain requests in realtime. Supervised and unsupervised algorithms such as random forest and neural networks help firewalls examine features like domain entropy, query patterns, and packet size to sort domains with a good accuracy rate. Such solutions provide timely protection against

unauthorized communication and ensure that such an organization is highly secure. Most of these solutions are based on a continuously fresh list of known malicious domains [37].

C. Using Encrypted DNS Services, Which Include DoH and DoT Protocols

DNS over HTTPS (DoH) and DNS over TLS (DoT) protect the DNS resolution process. which protects DNS requests from attackers who operate in the path. User privacy protection and defense against ISP-level DNS injection or eavesdropping occur through this set of security measures.

- With encryption, no one else can see the websites users access, including ISPs.
- They stop DNS injection and spoofing by checking that the DNS server is approved and that its answer has not been modified.
- TLS certificate validation is used to stop man-in-the-middle (MITM) attacks at each level.

D. Threat Intelligence Automation

As cyber dangers are still evolving, blending threat intelligence with high-quality artificial intelligence and machine learning tools is everything that is required to make DNS filtering protection stronger [38].

E. Using Reputable and Secure DNS Resolvers

DOI: https://doi.org/10.67535/tsp.000001.030

All individuals and organizations must use DNS services with built-in security features. People can access DNS encryption and threat blocking through Quad9, Cloudflare, and Google services.

F. Segmentation and Access Control

External DNS resolver access constraints enforced against DNS query senders stop malware from spreading laterally and illegal network usage. Implementing role-based access control (RBAC) for DNS management further reduces the risk of unauthorized changes.

G. Training and Awareness of Users

Advancements in the technology have forced the both performance and privacy impact of many default DNS encryption configurations; For one thing, as an example, Firefox's default configuration will automatically send all personal DNS queries conducted by users over to Cloudflare, which might bring more to user privacy concerns. The analysis shows that the general public remains unaware of these technological changes [39].

H. blockchain based Name servers

Decentralized name servers aim to take the place of or help the traditional DNS by using blockchain and distributed technologies. In contrast to centralized DNS systems, where records are handled by a few control points, decentralized DNS places these records across a network that is owned by many organizations, making it less vulnerable to failures and hacking.In the recent years, several blockchain-based name systems have appeared, offer more decentralization of namespace than DNS. The community at large is in a dilemma on which of these systems is best in offering decentralized control of internet namespace [40].

IV. Conclusion

Today's digital communication requires DNS to function as its first point of entry, which makes this system exceed its fundamental internet role. The widespread usage of DNS makes it both a hidden yet powerful tool for digital communication, although hackers benefit from its vulnerabilities. The DNS is victim of numerous types of threats, including DNS spoofing, DDoS attacks, and tunneling attacks,data breaches and operational failures, but can be mitigated by prioritizing DNS security and adapting the protection methodsat every level of infrastructure as ISP Level and country level.Securing DNS helps organizations maintain business operations, keep their important data safe, and stay compliant. Advances in both decentralization and user knowledge will help the DNS systems remain strong and secure for future internet usage.

References

[1] G. Schmid et al. "Thirty Years of DNS Insecurity: Current Issues and Perspectives." IEEE Communications Surveys Tutorials, 23 (2021): 2429-2459. https://doi.org/10.1109/comst.2021.3105741.

[2] O. V. D. Toorn et al. "Addressing the challenges of modern DNS a comprehensive tutorial." Comput. Sci. Rev., 45 (2022): 100469.

[3] Aminollah Khormali et al. "Domain Name System Security and Privacy: A Contemporary Survey." Comput. Networks, 185 (2020): 107699. https://doi.org/10.1016/j.comnet.2020.107699.

[4] Root Servers : Online at https://root-servers.org

[5] Lan Wei et al. "Whac-A-Mole: Six Years of DNS Spoofing." ArXiv, abs/2011.12978 (2020).

[6] S. Greenstein et al. "The Aftermath of the Dyn DDOS Attack." IEEE Micro, 39 (2019): 66-68.

[7] Sang-Yoon Chang et al. "Query-Crafting DoS Threats Against Internet DNS." 2020 IEEE Conference on Communications and Network Security (CNS) (2020): 1-9. https://doi.org/10.1109/CNS48642.2020.9162166.

[8] Jean-Yves Bisiaux et al. "DNS threats and mitigation strategies." Netw. Secur., 2014 (2014): 5-9. https://doi.org/10.1016/S1353-4858(14)70068-6.

[9] F. Alharbi, Y. Zhou, F. Qian, Z. Qian and N. Abu-Ghazaleh, "DNS Poisoning of Operating System Caches: Attacks and Mitigations," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2851-2863, 1 July-Aug. 2022, doi: 10.1109/TDSC.2022.3142331.

[10] R. Houser, S. Hao, Z. Li, D. Liu, C. Cotton and H. Wang, "A Comprehensive Measurement-based Investigation of DNS Hijacking," 2021 40th International Symposium on Reliable Distributed Systems (SRDS), Chicago, IL, USA, 2021, pp. 210-221, doi: 10.1109/SRDS53918.2021.00029.

[11] Akiwate, Gautam, et al. "Retroactive identification of targeted DNS infrastructure hijacking." Proceedings of the 22nd ACM Internet Measurement Conference. 2022.

[12] B. Savenko et al. "Detection DNS Tunneling Botnets." 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 1 (2021): 64-69. https://doi.org/10.1109/IDAACS53288.2021.9661022.

[13] Wang, Yue, et al. "A comprehensive survey on DNS tunnel detection." Computer Networks 197 (2021): 108322.

[14] C. D. Xuan, "Detecting APT Attacks Based on Network Traffic Using Machine Learning," in Journal of Web Engineering, vol. 20, no. 1, pp. 171-190, January 2021, doi: 10.13052/jwe1540-9589.2019.

[15] Harinahalli Lokesh, Gururaj, and Goutham BoreGowda. "Phishing website detection based on effective machine learning approach." Journal of Cyber Security Technology 5.1 (2021): 1-14.

[16] Julian Daffa Dzaky et al. "Improving DNS Server Resilience Against DDoS Attacks Through Anycast Routing." 2024 6th International Conference on Cybernetics and Intelligent System (ICORIS), Bandung, Indonesia, 2024, pp. 1-6, doi: 10.1109/ICORIS63540.2024.10903731.

[17] Bringer, Didier, and Lionel Tailhardat. "DSecO: Domain Name System (DNS) Data as a Knowledge Graph for Enhanced Security Analysis." (2025).

[18] 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.

[19] Elias Heftrig et al. "Poster: The Unintended Consequences of Algorithm Agility in DNSSEC." Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (2022). https://doi.org/10.1145/3548606.3563517.

[20] Lyu, Minzhao, Hassan Habibi Gharakheili, and Vijay Sivaraman. "A survey on DNS encryption: Current development, malware misuse, and inference techniques." ACM Computing Surveys 55.8 (2022): 1-28.

[21] Hounsel, P. Schmitt, K. Borgolte and N. Feamster, "Can encrypted DNS be fast?" in Passive and Active Measurement, Cham, Switzerland:Springer, pp. 444-459, 2021.

[22] K. Jerabek, O. Rysavy and I. Burgetova, "Measurement and characterization of DNS over HTTPS traffic", arXiv:2204.03975, 2022.

[23] 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.

[24] 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.

[25] Fejrskov, Martin, Emmanouil Vasilomanolakis, and Jens Myrup Pedersen. "A study on the use of 3rd party DNS resolvers for malware filtering or censorship circumvention." IFIP International Conference on ICT Systems Security and Privacy Protection. Cham: Springer International Publishing, 2022.

[26] D. F. F. Boeira, E. J. Scheid, M. F. Franco, L. Zembruzki and L. Z. Granville, "Traffic Centralization and Digital Sovereignty: An Analysis Under the Lens of DNS Servers," NOMS 2024-2024 IEEE Network Operations and Management Symposium, Seoul, Korea, Republic of, 2024, pp. 1-9, doi: 10.1109/NOMS59830.2024.10575700.

[27] Guanglin Duan et al. "DNSGuard: In-Network Defense Against DNS Attacks." IEEE Transactions on Dependable and Secure Computing, 22 (2025): 597-613. https://doi.org/10.1109/TDSC.2024.3409545.

[28] Tasnuva Mahjabin et al. "Load Distributed and Benign-Bot Mitigation Methods for IoT DNS Flood Attacks." IEEE Internet of Things Journal, 7 (2020): 986-1000. https://doi.org/10.1109/JIOT.2019.2947659.

[29] Delignat-Lavaud, Antoine, et al. "Transparent Attested DNS for Confidential Computing Services." arXiv preprint arXiv:2503.14611 (2025).

[30] Burrell, James. "Special issue on domain name system (DNS)." Journal of Cyber Policy 8.2 (2023): 137-141.

[31] Xu, Chengxi, et al. "Measuring the Centrality of DNS Infrastructure in the Wild." Applied Sciences 13.9 (2023): 5739.

[32] Chengxi Xu et al. "Measuring the Centrality of DNS Infrastructure in the Wild." Applied Sciences (2023). https://doi.org/10.3390/app13095739.

[33] Xue, Defan, et al. "APT attack detection scheme based on CK sketch and DNS traffic." Sensors 23.4 (2023): 2217.

[34] García, Sebastián, et al. "Large scale measurement on the adoption of encrypted DNS." arXiv preprint arXiv:2107.04436 (2021).

[35] Z. Xiao, Q. Sun and L. Tian, "DNS Route Tampering Attack in 5G Application Layer," 2024 IEEE 24th International Conference on Communication Technology (ICCT), Chengdu, China, 2024, pp. 863-871, doi: 10.1109/ICCT62411.2024.10946416.

[36] Kim, T. H.; Reeves, D. A survey of domain name system vulnerabilities and attacks. J. Surveill. Secur. Saf. 2020, 1, 34-60. http://dx.doi.org/10.20517/jsss.2020.14

[37] Marques, Claudio, Silvestre Malta, and João Magalhães. "DNS firewall based on machine learning." Future Internet 13.12 (2021): 309.

[38] Gladin, Issac, Vinodh Ewards, and Sebastian Terence. "Domain Name Server Filtering Service Using Threat Intelligence and Machine Learning Techniques." International Conference on Inventive Communication and Computational Technologies. Singapore: Springer Nature Singapore, 2024.

[39] Alexandra Nisenoff et al. "Understanding User Awareness and Behaviors Concerning Encrypted DNS Settings." Ar Xiv, abs/2208.04991 (2022).
DOI: https://doi.org/10.67535/tsp.000001.030
[40] Kocaogullar, Yekta, Eric Osterweil, and Lixia Zhang. "Towards a Decentralized Internet Namespace." Proceedings of the ACM Conext-2024 Workshop on the Decentralization of the Internet. 2024.