International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-5, September 2025
DOI: https:/doi.org/10.55524/ijircst.2025.13.5.1
Article ID IJIRE-1411, Pages 1-6
www.ijircst.org

A Systematic Review of the Impact of DNS-Layer Security Mechanisms on Internet Network Performance and Threat Mitigation

Noah K. Bamfo[1], **Christian Avornu**[2], **Abigail Nanayaa Otchill**[3], **Hassan Cessi Ibrahim**[4], **and Ramini Nikhil Sai**[5]

[1] Consulting Network Engineer, Networks and Security, IT Department, Lidl US, Arlington, Virginia, United States
[2, 4, 5] PG Scholar, J. W. McClure School of Emerging Communication Technologies, Ohio University, Athens, Ohio, United States
[3] Network Engineer, Foundation and Support team, Meta, Richmond, Virginia, United States

Correspondence should be addressed to Noah K. Bamfo; bamfokusinoah@gmail.com

Received 9 July 2025; Revised 24 July 2025; Accepted 10 August 2025

ABSTRACT- The Domain Name System (DNS) remains a foundational element of internet functionality, yet it is inherently vulnerable to various cyber threats due to its lack of built-in security features. In response, DNS-layer security mechanisms such as DNSSEC, DNS-over-TLS (DoT), and DNS-over-HTTPS (DoH) have been introduced to bolster security and privacy. However, the implementation of these protocols has raised concerns regarding their impact on network performance. This systematic review examines literature from 2015 to 2025, analyzing the dual effects of DNS-layer security on threat mitigation and network efficiency. Using a structured PRISMA-based methodology across six major academic databases, 23 peer-reviewed review articles were analyzed. The findings highlight the effectiveness of modern AI and ML-based approaches in enhancing encrypted DNS traffic detection, the performance trade-offs associated with encryption techniques, and the need for adaptive and privacy-aware security frameworks. The review also identifies key gaps and emerging trends, proposing directions for future research, including quantum-resilient systems and lightweight models for resource-constrained environments.

KEYWORDS- DNS Security, DNS-Layer Security, Network Performance, Payload Size, DNSSEC, DNS-over-TLS , Systematic Review

I. INTRODUCTION

The Domain Name System (DNS) is an essential component of modern internet infrastructure. It functions as a distributed directory, converting user-friendly domain names such as www.example.com into machine-readable IP addresses. Despite its pivotal role in enabling seamless communication across networks, DNS was not originally designed with security in mind[1]. As a result, it has become a significant attack vector, susceptible to threats such as cache poisoning, DNS spoofing, domain hijacking, and distributed denial-of-service (DdoS) attacks[2]. To mitigate these vulnerabilities, several DNS-layer security mechanisms have been introduced over the past two decades. Among the most prominent are DNS Security Extensions (DNSSEC), DNS-over-TLS (DoT), and DNS-over-HTTPS (DoH). DNSSEC adds a layer of authenticity by digitally signing DNS records, preventing tampering and impersonation[3], [4]. DoT and DoH, on the other hand, encrypt DNS traffic between clients and resolvers to ensure confidentiality and prevent surveillance or manipulation by intermediaries.

While these mechanisms strengthen the security posture of DNS communications, their adoption has introduced concerns regarding performance degradation. Specifically, the introduction of encryption and cryptographic validation processes can lead to increased query latency, larger payload sizes, and higher computational overhead[5]. These changes have prompted a crucial question in network security and performance engineering: Does DNS-layer security meaningfully impact network performance, and if so, how? Recent studies have attempted to evaluate the trade-offs between enhanced security and network efficiency. For example, encrypted DNS protocols like DoH, which encapsulate DNS queries in HTTPS packets, offer improved privacy but have been observed to introduce additional latency due to TLS handshakes and HTTP/2 overhead[6], [7]. Conversely, DNSSEC implementations, while effective in ensuring data integrity, may suffer from scalability limitations and increased DNS response sizes that strain network bandwidth and resolver infrastructure.

Despite ongoing discourse and several empirical studies, there remains a lack of consolidated evidence and systematic analysis concerning the overall impact of DNS-layer security mechanisms on network performance[8], [9], [10]. Furthermore, the diversity of experimental setups, performance metrics, and security objectives in existing literature complicates the ability to draw generalizable conclusions. Some studies focus primarily on latency metrics, while others emphasize throughput, packet loss, or CPU utilization, leading to fragmented insights.

To understand the current landscape and future directions of DNS-Layer Security, we conducted a systematic review of the literature from the past ten years (2015-2025). This review focuses on identifying key trends, advancements, and challenges in the application of DNS-Layer security. By examining review papers from five leading academic databases—Google Scholar, MDPI, Science Direct, Springer, and IEEE—we aimed to capture a comprehensive overview of developments in this field. This review aims to fill the knowledge gap by: Identifying and analyzing peer-reviewed studies that evaluate the performance implications of DNS-layer security technologies; Examining the extent to which security measures such as DNSSEC, DoH, and DoT affect network parameters such as latency, payload size, throughput, and query success rate; Investigating the effectiveness of these mechanisms in mitigating common DNS-based attacks.

The remainder of the document is structured as follows: The methodology used for the systematic review is presented in Section II, along with the number of articles per database source, the inclusion and exclusion criteria, and the publication selection procedure. The review of the chosen publications is presented in Section III. Section IV included the review's conclusions and recommendations for future lines of inquiry. The paper is concluded in Section V.

II. RESEARCH METHOD

This section presents a systematic review of the role of AI in cybersecurity from 2014 to August 2024, focusing solely on review articles. The PRISMA methodology guided the review process, utilizing six academic databases: MDPI, Springer, Science Direct, Elsevier, IEEE Xplore, and Google Scholar, to source reliable, peer-reviewed publications. The search string used was: (“DNS-layer security” OR “DNSSEC” OR “DNS-over-TLS”) AND (“network performance” OR “latency” OR “throughput”) AND (“cyber threats” OR “attack mitigation”) to identify relevant reviews. Duplicates were avoided by tracing Google Scholar results back to their original journals. Table I details the inclusion and exclusion criteria, while Figure 1 outlines the publications selection process.

Table 1: Inclusion and exclusion criteria

Included	Excluded
Review publications focusing on the role of DNS-Layer security, including performance and Threat, based on year, title, abstract and full text.	Non-review journal articles, book chapters, and conference proceedings.
Studies written in English	Studies not written in English
Peer-reviewed review articles, book chapters, and conferences proceedings from any of the considered database sources	Non-peer-reviewed publications such as pre-prints.
Open-access review publications or publications available through the researcher's institution's subscriptions	Publications not accessible through the researcher's institution's subscriptions or with restricted access
Revie articles published between 2015 and May 2025	Review articles published before 2015

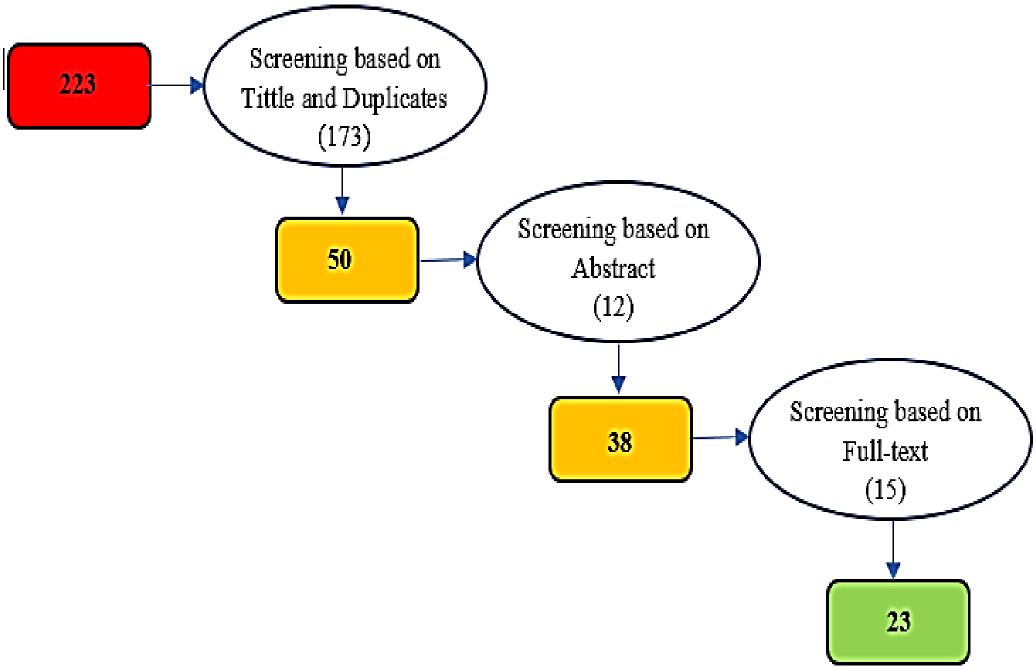
223
Screening based on Tittle and Duplicates (173)
50
Screening based on Abstract (12)
38
Screening based on Full-text (15)
23

Figure 1: The Article Selection Process

In the below Figure 2 (bar graph) shows the number of articles obtained after considering relevance of research papers with the subjected objectives.

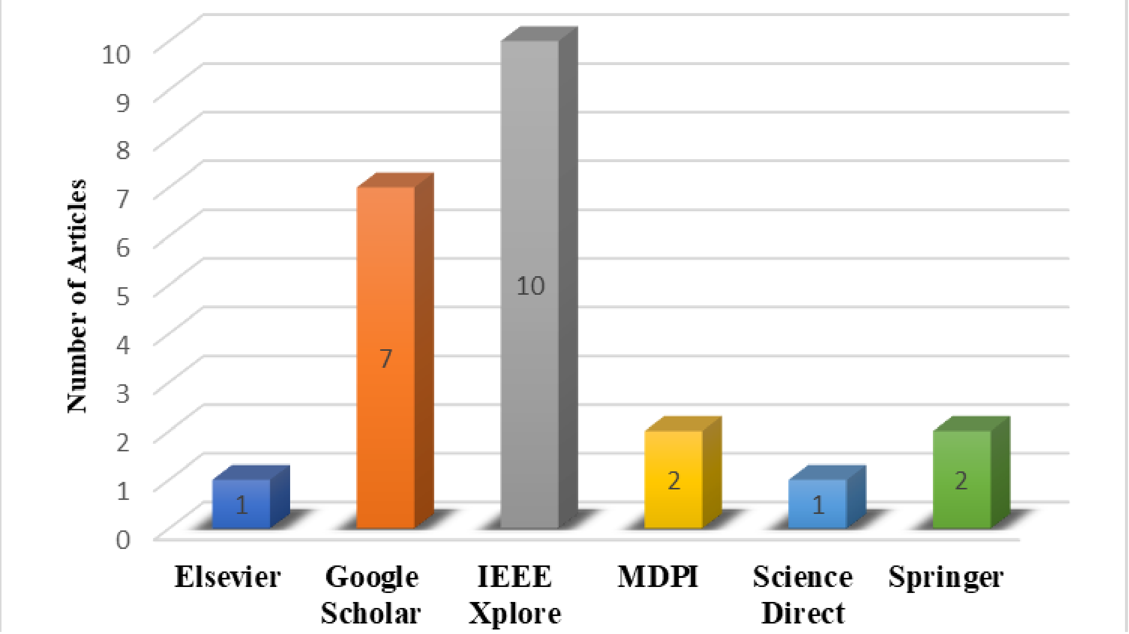

Figure 2: Number of Article Per Database Source

III. REVIEW OF EXISTING REVIEW WORKS

A. DNS-Layer security Developments and Performance

The technologies for identifying harmful requests in computer networks and implementing malicious request detection systems based on them have been examined in related literatures [11], [12]. With an emphasis on how encryption affects DNS query performance and resolver efficiency, these studies assess the performance impact of various cryptographic algorithms, including Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) 128 and ChaCha20-Poly1305, within the DoT architecture. Several cryptographic algorithms were used in performance tests with varying client load scenarios. To evaluate how encryption affected DNS recursive resolvers, metrics like response rate, timeout rate, and resource usage were examined. Additionally, [4], [7] offers a thorough examination of how DoH weaknesses affect cybersecurity. Talking about different methods for identifying DoH tunnelling and emphasizing the necessity of ongoing research and development to guarantee the efficacy of DoH as a tool for enhancing security and privacy.

A Selective Re-Query (SRQ) Case Sensitive Encoding scheme to efficiently prevent DNS cache poisoning attacks was proposed by [13].The scheme also kept the network efficiency nearly at the minimal level. Additionally, [14], [15] discussed DNS poisoning methods that target the client-side DNS cache. In order to get beyond defenses that target resolvers, the attack starts DNS poisoning on the client cache, which is utilized in all mainstream operating systems to enhance DNS performance. However, in practice, the suggested methods are more attractive for defending the DNS solely against cache poisoning attacks.

A comprehensive study on DNS privacy and security, was performed on article [14] which analyses the limitations as well as strengths of utilized data analysis methods which offered valuable guideline to analyze the existing challenges such Amplification and Dos Attack, DNS Cache Poisoning, Botnet and Attacks using DNS, Phishing Attacks, DNS Manipulations, Malicious Domains Detections, Domain Generation Algorithm, Domain Name Squatting, Packed Domain Monetization ,Privacy leakage in DNS ecosystem. In [15],solution to protect networks from these large DNS amplification attacks was proposed. The solution involves a set of geographically distributed routers, called a Barrier of Routers (BoR). The barrier scans all incoming traffic, drops attack traffic and sends the rest to the intended recipient. [16] uses Deep Packet Inspection (DPI) to apply filtering rules and block harmful domains. Network administrators can use programmable switches for security controls. This method can parse more domain labels and improves throughput, delay, and packet loss compared to traditional firewalls. It uses minimal resources for additional security features. Furthermore, the authors in [17] propose a privacy-aware schema that allows Authoritative DNS Servers to distribute their zones to third parties without disclosing sensitive information, enabling effective DNS attack mitigation. The schema uses Cuckoo Filters' space, time, and privacy properties for efficient zone mapping, preserving privacy.

The research in [18], [19] proposes a client-based DNSSEC validation and alarm system to transfer the validation process from the DNS full resolver to each querying client. The system also includes an adaptive alarm mechanism, alerting users of failure messages and responses. This approach reduces workload on DNS full resolvers and encourages DNSSEC deployment by resolving existing issues. However, both systems have limitations in performance evaluation and tuning in real network environments. A Distributed Rate Sharing based Amplified DNS-DdoS Attack Mitigation (DRSADAM) was introduced in [20], a DNS-DdoS attack mitigation technique that shares DNS query rates among attack participants, ensuring peak attack rates remain below a victim's threshold, and taking only a few seconds to complete.

A novel practical and powerful pulsating DoS attack DNSBOMB was proposed in [21]. DNSBOMB uses a variety of widely used DNS techniques to collect low-rate DNS queries, magnify them into large-sized responses, then concentrate all DNS responses into a short, high-volume periodic pulsing burst to simultaneously overwhelm target systems. DNSBOMB outperforms prior DoS attacks, with a peak pulse magnitude of 8.7Gb/s and a bandwidth amplification factor of more than 20,000. Their experimental results revealed that DNSBOMB causes full packet loss and service degradation. Information-based Heavy Hitters (ibHH) was proposed in [22], ibHH a real-time detection technique based on real-time estimates of the volume of data sent to registered domains. In order to further decrease detection and response time, ibHH can be deployed on recursive DNS servers because it uses constant-size memory and allows constant-time queries. Here, efficacy was not taken into account.

The research in [23] presents TITAN-DoH, a mathematically rigorous, trust-enriched system that redefines DNS security as a dynamic, context-aware, and post-quantum-resilient mesh. It includes a five-pillar multilayered security framework, including a Trust Algebra, Graph Signal Processing, Bayesian Contextual Engines, FrodoKEM-strengthened TLS handshakes, and Verifiable Delay Functions for temporal query authentication and replay attack protection. NinjaDoH, a new DNS over HTTPS protocol, uses public cloud infrastructure and the Inter Planetary Name System (IPNS) to create a moving target DoH service impervious to censorship[24]. This strong, moving target DNS solution ensures uninterrupted, safe internet access in settings with strong DNS-based filtering. The DNS system in F20 was disrupted by the NoneXistent Name Server Attack (NXNSAttack), causing difficulties for internet users to access websites and online resources. The attack creates a storm of packets between authoritative name servers and resolvers, causing a storm. To lessen the attack's impact, an improvement to the recursive resolver algorithm, MaxFetch(k), is suggested. This work focuses on communications between recursive resolvers and authoritative structures [25].

B. ML and AI Approach to DNS-Layer security

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into DNS-layer security has significantly enhanced the ability to detect, predict, and mitigate domain-based threats in real-time.

The study referenced in [26] presents a DNS over HTTPS (DoH) Tunneling Detection System that leverages a selective feature approach optimized through Ant Colony Optimization (ACO). The researchers address the limitations of DNSSEC by developing an enhanced dual-path feature selection strategy aimed at identifying the most relevant packet features for both binary classification (distinguishing between DoH-Normal and DoH-Malicious) and multiclass classification (Non-DoH, DoH-Normal, DoH-Malicious). ACO is combined with ML models such as XGBoost, K-Nearest Neighbors (KNN), Random Forest (RF), and Convolutional Neural Networks (CNNs), with the CIRACIC-DoHBrw-2020 dataset used for evaluation. The findings demonstrate that the proposed system effectively identifies optimal features, resulting in superior detection accuracy compared to prior intrusion detection systems (IDS). Additionally, the streamlined feature set significantly reduces computational load and processing time across all applied classifiers, offering a fast, accurate, and efficient solution for handling encrypted DNS traffic.

In [27], the authors introduce MTL-DoHTA, a multi-task learning framework for analyzing DNS over HTTPS (DoH) traffic. It performs three key classification tasks: distinguishing DoH from non-DoH traffic, detecting benign versus malicious DoH, and identifying specific DNS tunneling tools like dns2tcp, dnscat2, and iodine. Using statistical traffic features and a 2D-CNN model enhanced with GradNorm and attention mechanisms, MTL-DoHTA achieves a high macro-average F1-score of 0.9905 on the CIRA-CIC-DoHBrw-2020 dataset. The framework proves to be an effective and efficient solution for securing sensor-based networks against advanced DNS threats, particularly in environments with limited resources. Paper [28] explores the impact of DoH in the gaming industry, focusing on the balance between user privacy and threat detection. The authors propose a hybrid framework that enhances privacy using encrypted DNS while enabling threat detection through on-device monitoring, behavioral analysis, and machine learning. By analyzing DNS query patterns and integrating real-time threat intelligence, the framework accurately identifies risks such as DNS tunneling, phishing, and abnormal DoH traffic without decrypting queries. This ensures strong security with minimal latency and without compromising player privacy. The study underscores the need for adaptive security solutions in gaming platforms as encrypted DNS usage becomes more widespread. Article [29] investigates whether Server Name Encryption (SNE) truly safeguards user privacy. The study demonstrates that even with encrypted domain names, attackers monitoring network traffic can still infer visited websites using basic features and standard ML models. Using large-scale network traces, the authors examine multiple attack scenarios, including identifying individual domain queries, reconstructing users' browsing histories, and determining which users access specific websites. Additional scenarios involve extracting domain lists and estimating website audiences. The research also evaluates the effectiveness of padding techniques and explores using data from automated crawlers for training. Findings reveal that domain name encryption alone does not ensure privacy and may give users a false sense of security, emphasizing the limitations of solutions like DoH and Encrypted Client Hello (ECH).

Paper [30] presents a comprehensive AI-driven approach to enhancing DNSSEC security over DNS over HTTPS (DoH). It introduces a robust detection framework that integrates Capsule Networks (CapsNets), Graph Transformers, and Contrastive Self-Supervised Learning (CSSL) to detect advanced cyber threats in real time. The system is designed for resilience, interpretability, and speed, addressing key challenges in encrypted traffic analysis. CapsNets capture hierarchical patterns in DoH traffic, Graph Transformers detect temporal anomalies, and CSSL enables learning from unlabeled data. The framework not only improves encrypted traffic security but also sets a foundation for protecting emerging protocols like QUIC and HTTP/3. The findings confirm the effectiveness of AI-based, privacy-preserving methods in mitigating modern cyber threats and suggest that future integration with quantum-classical AI systems could further enhance threat detection in fast, encrypted networks.

IV. INSIGHT AND FURTHER RESEARCH DIRECTIONS

The systematic review reveals several critical insights and future research avenues across three primary domains:

A. Domain 1. Performance Trade-offs of DNS Security Mechanisms

DNS-layer security protocols such as DNSSEC, DoH, and DoT provide essential protections against spoofing, cache poisoning, and surveillance. However, their encryption and verification processes introduce increased latency, larger payload sizes, and added computational overhead. Studies comparing cryptographic algorithms like AES-GCM and ChaCha20 in different network loads highlight this trade-off, especially in high-throughput environments and latency-sensitive applications (e.g., real-time gaming, IoT). Future research should explore:

- Optimization of cryptographic operations to minimize performance penalties.
- Lightweight encryption protocols suitable for edge devices and constrained networks.
- Adaptive resolution strategies that dynamically balance performance and privacy based on contextual network parameters.

B. Domain 2. Efficacy of AI and ML in DNS Threat Detection

Recent advances demonstrate the promise of AI-driven models in improving DNS-layer security. Techniques including Capsule Networks, Graph Transformers, and Contrastive Self-Supervised Learning (CSSL) have enabled accurate and efficient classification of DNS traffic—even in encrypted environments like DoH. For instance, the use of Ant Colony Optimization in feature selection, multi-task learning models (e.g., MTL-DoHTA), and privacy-aware monitoring frameworks have shown high accuracy in real-time detection of tunneling, phishing, and malware domains. Potential research directions include:

- Federated learning and reinforcement learning for decentralized, privacy-preserving threat detection.
- AI-enhanced payload obfuscation detection without breaking encryption.
- Quantum-augmented AI models for processing large-scale DNS traffic with improved anomaly detection precision.

C. Domain 3. Limitations of Current Privacy Enhancements

Contrary to popular assumptions, mechanisms such as Server Name Encryption (SNE), DoH, and ECH may not fully ensure privacy. Adversaries can still infer domain names and user behavior using traffic pattern analysis and off-the-shelf ML tools. Studies demonstrate high success rates in identifying domain access from encrypted streams using large-scale traffic traces. This gap calls for:

- Advanced traffic padding and obfuscation techniques that mitigate metadata leakage.
- Real-time traffic pattern analysis countermeasures integrated into client-side resolvers.
- Hybrid DNS architectures that combine centralized control with decentralized privacy enforcement.

V. CONCLUSION

This systematic review offers a comprehensive synthesis of developments in DNS-layer security from 2015 to 2025, highlighting both its strengths in threat mitigation and its challenges in maintaining optimal network performance. While protocols like DNSSEC, DoT, and DoH significantly enhance internet security, they introduce performance overheads that must be carefully managed—especially in latency-sensitive and resource-constrained environments. The integration of AI and ML has emerged as a transformative force, enabling real-time detection of complex threats in encrypted traffic. However, persistent privacy vulnerabilities and the need for lightweight, adaptive models highlight areas where further innovation is crucial.

To advance the field, future research should focus on developing resilient, efficient, and privacy-preserving DNS security frameworks. This includes exploring hybrid quantum-classical AI systems, optimizing cryptographic protocols for speed and scalability, and reinforcing user anonymity against increasingly sophisticated traffic analysis techniques. As the internet transitions toward more encrypted and decentralized architectures, robust DNS-layer security will remain a cornerstone of cyber resilience and trust.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

1. Ayoub, S. Balakrichenan, K. Khawam, and B. Ampeau, "DNS for IoT: A Survey," *Sensors*, vol. 23, no. 9, p. 4473, May 2023. Available from: https://hal.science/hal-04106348/document
2. T. Rebekah, "Four major DNS attack types and how to mitigate them," *Bluecat*. Accessed: May 31, 2025. Available from: https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/
3. G. Schmid, "Thirty Years of DNS Insecurity: Current Issues and Perspectives," *IEEE Communications Surveys & Tutorials*, vol. PP, p. 1, May 2021. Available from: https://ieeexplore.ieee.org/abstract/document/9520679
4. M. Dawood et al., "The Impact of Domain Name Server (DNS) over Hypertext Transfer Protocol Secure (HTTPS) on Cyber Security: Limitations, Challenges, and Detection Techniques," *Computers, Materials & Continua*, vol. 80, no. 3, pp. 4513–4542, 2024. Available from: https://doi.org/10.32604/cmc.2024.050049
5. N. Abosata, S. Al-Rubaye, and G. Inalhan, "Lightweight Payload Encryption-Based Authentication Scheme for Advanced Metering Infrastructure Sensor Networks," *Sensors*, vol. 22, no. 2, p. 534, Jan. 2022. Available from: https://doi.org/10.3390/s22020534
6. G. Kambourakis and G. Karopoulos, "Encrypted DNS: The good, the bad and the moot," *Computer Fraud & Security*, vol. 2022, no. 5, May 2022. Available from: https://doi.org/10.12968/S1361-3723(22)70572-6
7. K. Bumanglag and H. Kettani, "On the Impact of DNS Over HTTPS Paradigm on Cyber Systems," in *Proc. 3rd Int. Conf. Information and Computer Technologies (ICICT)*, IEEE, Mar.

2020, pp. 494–499. Available from: https://doi.org/10.1109/ICICT50521.2020.00085

8. R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic Literature Review on Security Risks and its Practices in Secure Software Development," *IEEE Access*, vol. 10, pp. 5456–5481, 2022. Available from: https://ieeexplore.ieee.org/abstract/document/9669954
9. R. Curtmola, A. Del Sorbo, and G. Ateniese, "On the Performance and Analysis of DNS Security Extensions," 2005, pp. 288–303. Available from: https://link.springer.com/chapter/10.1007/11599371_24
10. R. Radu and M. Hausding, "Consolidation in the DNS resolver market – how much, how fast, how dangerous?," *Journal of Cyber Policy*, vol. 5, no. 1, pp. 46–64, Jan. 2020. Available from: https://doi.org/10.1080/23738871.2020.1722191
11. O. O. Blaise, A. Wumi, and U. Alfred, "Enhancing DNS Performance with Efficient Cryptographic Algorithms: A Comparative Study of DoT Frameworks," *Asian Journal of Computer Science and Technology*, vol. 13, no. 2, pp. 48–55, Nov. 2024. Available from: https://doi.org/10.70112/ajcst-2024.13.2.4288
12. O. Leshchenko, O. Trush, M. Trush, A. Horachuk, and O. Makhovych, "Technologies for Detecting Malicious Requests in Computer Networks Based on the DNS Protocol," 2023. Available from: https://ceur-ws.org/Vol-3646/Short_4.pdf
13. J. Cao, M. Ma, X. Wang, and H. Liu, "A Selective Re-Query Case Sensitive Encoding Scheme Against DNS Cache Poisoning Attacks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1263–1279, Jun. 2017. Available from: https://doi.org/10.1007/s11277-016-3681-2
14. Khormali et al., "Domain name system security and privacy: A contemporary survey," *Computer Networks*, vol. 185, p. 107699, Feb. 2021. Available from: https://doi.org/10.1016/j.comnet.2020.107699
15. Gupta and E. Sharma, "Mitigating DNS Amplification Attacks Using a Set of Geographically Distributed SDN Routers," in *Proc. Int. Conf. Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, Sep. 2018, pp. 392–400. Available from: https://doi.org/10.1109/ICACCI.2018.8554459
16. AlSabeh, E. Kfoury, J. Crichigno, and E. Bou-Harb, "P4DDPI: Securing P4-Programmable Data Plane Networks via DNS Deep Packet Inspection," *Internet Society*, Feb. 2023. Available from: https://doi.org/10.14722/madweb.2022.23012
17. N. Kostopoulos, D. Kalogeras, and V. Maglaris, "Enabling Privacy-Aware Zone Exchanges Among Authoritative and Recursive DNS Servers," in *Proc. Applied Networking Research Workshop*, ACM, Jul. 2020, pp. 1–8. Available from: https://doi.org/10.1145/3404868.3406665
18. K. Kakoi et al., "Design and Implementation of a Client Based DNSSEC Validation and Alert System," in *Proc. IEEE 40th Annual Computer Software and Applications Conf. (COMPSAC)*, Jun. 2016, pp. 8–13. Available from: https://doi.org/10.1109/COMPSAC.2016.91
19. Y. Jin et al., "A Client Based DNSSEC Validation System with Adaptive Alert Mechanism Considering Minimal Client Timeout," *IEICE Transactions on Information and Systems*, vol. E100.D, no. 8, pp. 1751–1761, 2017. Available from: https://doi.org/10.1587/transinf.2016ICP0028
20. S. Verma et al., "Stopping Amplified DNS DDoS Attacks through Distributed Query Rate Sharing," in *Proc. 11th Int. Conf. Availability, Reliability and Security (ARES)*, IEEE, Aug. 2016, pp. 69–78. Available from: https://doi.org/10.1109/ARES.2016.93
21. X. Li, D. Wu, H. Duan, and Q. Li, "DNSBomb: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses," in *Proc. IEEE Symposium on Security and Privacy (SP)*, May 2024, pp. 4478–4496. Available from: https://doi.org/10.1109/SP54263.2024.00264
22. Y. Ozery, A. Nadler, and A. Shabtai, "Information Based Heavy Hitters for Real-Time DNS Data Exfiltration Detection," *Internet Society*, Feb. 2024. Available from: https://doi.org/10.14722/ndss.2024.24388
23. Ali and G. Chen, "TITAN-DoH: Trust-Integrated Threat Adaptive Network for Post-Quantum Secure DNS over HTTPS." Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5230452
24. S. Seidenberger et al., "NinjaDoH: A Censorship-Resistant Moving Target DoH Server Using Hyperscalers and IPNS," 2024. Available from: https://doi.org/10.48550/arXiv.2411.02805
25. S. Lior, A. Yehuda, and A. Bremler-Barr, "NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities," *USENIX Conference*, 2020. Available from: https://www.usenix.org/system/files/sec20_slides_afek.pdf
26. H. S. Talabani, Z. K. Abdul, and H. M. M. Saleh, "DNS over HTTPS Tunneling Detection System Based on Selected Features via Ant Colony Optimization," *Future Internet*, vol. 17, no. 5, p. 211, May 2025. Available from: https://doi.org/10.3390/fi17050211
27. W. K. Jung and B. I. Kwak, "MTL-DoHTA: Multi-Task Learning-Based DNS over HTTPS Traffic Analysis for Enhanced Network Security," *Sensors*, vol. 25, no. 4, Feb. 2025. Available from: https://doi.org/10.3390/s25040993
28. S. Talwar, "DNS over HTTPS (DoH) in Gaming: Balancing Privacy and Threat Visibility." Available from: https://www.researchgate.net/publication/389167512
29. M. Trevisan et al., "Attacking DoH and ECH: Does Server Name Encryption Protect Users' Privacy?," *ACM Transactions on Internet Technology*, vol. 23, no. 1, pp. 1–22, Feb. 2023. Available from: https://doi.org/10.1145/3570726
30. Ali, "Next-Generation AI for Advanced Threat Detection and Security Enhancement in DNS Over HTTPS," 2025. Available from: https://doi.org/10.2139/ssrn.5224919