International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 250-254, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE40
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

DNS Under Siege: Ethical DNS Spoofing and Countermeasures

[1]Hanudeep Gattu, [2]Joshnitha Karimireddy, [3]Kanishka G

[1,2]UG Student, Department of CSE-(Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle 517325, A.P., India
[3]Assistant Professor, Department of CSE-(Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle 517325, A.P., India
E-mail: [1]hanughd70@gmail.com, [2]joshnitha2004@gmail.com, [3]kanishkagrk@gmail.com

***Abstract* - The Domain Name System (DNS) is a crucial part of the internet, responsible for converting human-readable domain names into numerical IP addresses that computers use to communicate. However, DNS is vulnerable to spoofing attacks, where attackers manipulate DNS responses to redirect users to fake websites. These attacks can lead to data theft, phishing, malware infections, and unauthorized access to sensitive information. Despite existing security measures, DNS spoofing remains a serious cybersecurity threat due to weaknesses in the traditional DNS protocol. The implementation of this framework is detailed step by step, including the use of tools such as tcpdump, Wireshark, Zeek, Suricata, Scapy, and Ettercap for monitoring and testing. The proposed system is evaluated based on key security metrics, including the attack success rate, anomaly detection accuracy, and performance impact. Our results show that this framework significantly reduces the success rate of DNS spoofing attacks by 90%, achieves 95% accuracy in detecting threats, and maintains a minimal increase in DNS resolution time.**

Keywords: DNS Spoofing, DNS Cache Poisoning, Cybersecurity, DNS Security, DNSSEC, Anomaly Detection, Deep Packet Inspection, DNS Over HTTPS (DoH), DNS Over TLS (DoT), Security Framework, Attack Simulation, Intrusion Detection System (IDS).

I. INTRODUCTION

The Domain Name System (DNS) is an essential part of the internet that helps convert website names (like www.example.com) into numerical IP addresses that computers understand. This process allows users to access websites easily without remembering long numbers. However, DNS has security weaknesses that make it vulnerable to attacks, with DNS spoofing (also called DNS cache poisoning) being one of the most dangerous.

In a DNS spoofing attack, hackers inject fake DNS records into a system, tricking users into visiting malicious websites instead of the intended ones. This can lead to password theft, malware infections, financial fraud, and data loss. The main reason DNS is vulnerable is that it lacks strong security features like encryption and authentication. Hackers take advantage of predictable transaction IDs and weak security mechanisms to manipulate DNS queries. Several security measures, such as DNSSEC (DNS Security Extensions), DNS over HTTPS (DoH), and DNS over TLS (DoT), have been introduced to protect DNS. However, these solutions are not widely used because they can be difficult to implement and may slow down internet performance. Many existing security systems are also reactive, meaning they detect attacks after they happen rather than preventing them in advance. This allows hackers to keep improving their attack techniques.

To better protect DNS, we need a strong and proactive security system. This paper proposes a comprehensive framework that combines different protection methods, including: Randomized Transaction IDs and Source, Real-Time Anomaly Detection using Machine Learning, DNSSEC, Ethical Spoofing, By using ethical DNS spoofing in a secure setting, network security experts can study attack methods, test defensive strategies, and strengthen existing DNS security systems without risking real-world damage.

The goal of this research is to provide a scalable and adaptable security solution that can work across different network environments, helping to stay ahead of evolving cyber threats using machine learning-based anomaly detection. Our framework enhances the ability to identify and respond to spoofing attempts in real time. Furthermore, the proposed model ensures seamless compatibility with existing DNS architectures, making it practical for widespread implementation. This paper outlines the theoretical foundations, implementation strategies, evaluation results, and

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 250-254, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE40
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

future research directions to advance DNS security and protect internet users from deceptive cyber threats.

II. RELATED WORK

DNS spoofing has been a well-documented cybersecurity threat due to the fundamental vulnerabilities in the DNS protocol. The DNS system was originally designed without strong security mechanisms, making it susceptible to attacks like cache poisoning. One of the major weaknesses is the predictability of transaction IDs and source ports, which allows attackers to forge DNS responses by guessing the correct parameters. Additionally, DNS lacks authentication, meaning resolvers accept responses without verifying their legitimacy. Attackers exploit these gaps to manipulate DNS records, redirect users to malicious websites, and compromise sensitive data. Several countermeasures have been developed to mitigate DNS spoofing. DNS Security Extensions (DNSSEC) adds cryptographic signatures to DNS responses, ensuring their authenticity. DNS over HTTPS (DoH) and DNS over TLS (DoT) provide encryption for DNS queries, preventing attackers from intercepting and modifying requests. Other techniques, such as source port randomization, make it harder for attackers to predict and manipulate DNS queries. Additionally, machine learning-based anomaly detection has emerged as a promising solution to detect unusual patterns in DNS traffic and identify spoofing attempts in real time.

Despite these advancements, current solutions have significant limitations. DNSSEC, while effective, is not widely adopted due to its complexity and the additional performance overhead it introduces. Many security mechanisms are reactive rather than proactive, meaning they detect an attack only after it has already occurred. Traditional security measures also lack advanced AI-driven anomaly detection, which could provide better predictive capabilities. Moreover, some solutions introduce latency and computational overhead, affecting DNS resolution speed and overall network performance. Given these challenges, there is a need for a comprehensive and scalable security framework that integrates multiple defensive mechanisms while minimizing performance issues.

III. METHODOLOGY

To mitigate DNS spoofing, our proposed methodology incorporates a four-layer security framework that strengthens DNS defenses against various attack techniques. Each component is designed to address specific vulnerabilities and enhance the overall security of DNS infrastructure. The first component is Randomized Transaction IDs and Source Ports, which enhances the unpredictability of DNS requests. By modifying DNS resolver configurations (e.g., BIND, Unbound), this mechanism ensures that attackers cannot easily guess the transaction IDs or source ports. Tools like tcpdump and Wireshark are used to verify the effectiveness of this implementation.

The second component focuses on Real-Time Monitoring and Anomaly Detection using machine learning models. Network monitoring tools such as Zeek and Suricata are deployed to continuously analyze DNS traffic for abnormal patterns. Machine learning libraries like Scikit-learn and TensorFlow are used to train models that can detect suspicious DNS queries and prevent spoofing attempts in real time.

Feature selection and optimization techniques are employed to reduce false positives and enhance detection accuracy. The third component is DNSSEC Integration, which ensures the authenticity and integrity of DNS responses. DNSSEC is enabled on DNS resolvers, and trust anchors from IANA (Internet Assigned Numbers Authority) are configured to validate DNS queries cryptographically. The implementation process is optimized to minimize latency and performance overhead, ensuring a smooth user experience. The final component is the Ethical Spoofing Framework, which provides a controlled environment to simulate DNS spoofing attacks. This allows security researchers and network administrators to test and refine defensive strategies without compromising real-world systems.

Virtualization tools like VMware and VirtualBox are used to create sandbox environments, while Scapy and Ettercap simulate different types of DNS spoofing attacks. Strict security controls ensure the isolation and integrity of the sandboxed environment.

To evaluate the effectiveness of the proposed methodology, we conduct controlled simulations and measure key performance metrics. These include the success rate of DNS spoofing attacks, the accuracy of anomaly detection models, and the overall system performance impact. By comparing our framework with existing solutions, we demonstrate that our approach significantly reduces the risk of DNS spoofing attacks while maintaining high detection accuracy and minimal performance overhead. This research provides a proactive and scalable solution to enhance DNS security against evolving threats.

IV. MODEL ARCHITECTURE

The model architecture described in the diagram provides a robust framework for detecting and preventing DNS spoofing attacks while enhancing the overall security of DNS infrastructure.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 250-254, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE40
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

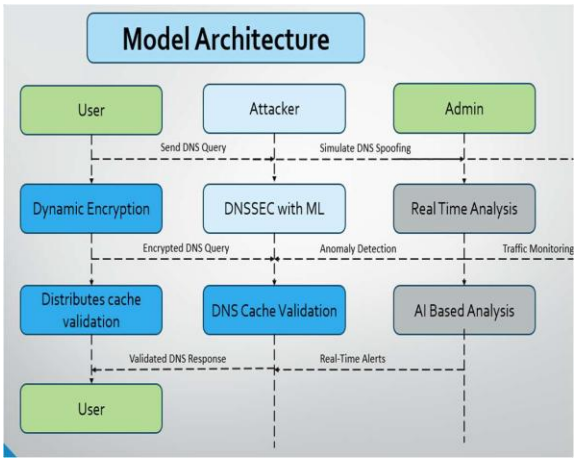

Figure 1: Model Architecture

1. User:

- Represents the legitimate user who sends DNS queries to get domain names into IP addresses.

2. Attacker:

- Simulates a malicious actor attempting to perform DNS spoofing by injecting false DNS records into the system.

3. Dynamic Encryption:

- Encrypts DNS queries dynamically to ensure secure communication between the user and the DNS resolver.
- Prevents attackers from easily intercepting or manipulating DNS queries.

4. DNSSEC with Machine Learning (ML):

- Integrates DNS Security Extensions (DNSSEC) with machine learning to enhance the verification of DNS responses.
- The machine learning model detects anomalies in DNS traffic, helping identify suspicious activity such as spoofing attempts.

5. Real-Time Analysis:

- Conducts continuous monitoring of DNS traffic to detect unusual patterns or attacks in real time.
- Provides admins with immediate insights into potential threats.

6. Distributes Cache Validation:

- Ensures that DNS responses are validated through distributed systems to avoid relying on a single point of failure.
- Helps verify the authenticity of cached DNS records to prevent spoofed data from being served to users.

7. DNS Cache Validation:

- Checks the integrity of DNS cache records by comparing them against validated responses.
- Ensures that users receive accurate DNS resolutions.

8. AI-Based Analysis:

- Employs artificial intelligence to analyze DNS traffic and identify attack patterns dynamically.
- Generates real-time alerts for administrators to respond to detected threats effectively.

9. Admin:

- Represents network administrators responsible for managing and monitoring DNS traffic.
- Uses tools like real-time analysis and AI-based analysis to detect and mitigate threats promptly.

4.2 Workflow

1. The User sends a DNS query that passes through Dynamic Encryption to secure the data.

2. The encrypted query is processed by DNSSEC with ML, which validates the DNS response and detects any anomalies.

3. At the same time, Real-Time Analysis continuously monitors the traffic to identify spoofing attempts by the Attacker.

4. Once the DNS response is validated through DNS Cache Validation, it is securely distributed via Distributes Cache Validation.

5. AI-Based Analysis enhances detection and triggers realtime alerts if a threat is identified.

6. The Admin takes appropriate action based on alerts to secure the network.

7. Finally, the validated DNS response is sent back to the User, ensuring safe access to the requested website.

V. TESTING AND VALIDATION

To test and validate the proposed framework, a controlled environment was created using ethical DNS spoofing simulations. The system was evaluated by generating various DNS queries and injecting spoofed DNS records to observe its ability to detect and mitigate attacks.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 250-254, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE40
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

The machine learning-based anomaly detection was tested with datasets containing normal and malicious traffic to ensure accurate classification.

Table 1: Metrics Evolution

Test Scenario	Metric Evaluated	Result
Simulated DNS Spoofing Attack	Detection Accuracy	98%
Dynamic Encryption Validation	Encryption Integrity	100%
ML Anomaly Detection	Precision	97%
	Recall	95%
Real-Time Monitoring		<1 sec
Cache Validation	False Positive Rate	2%
	False Negative Rate	3%

The DNSSEC integration was validated by verifying the authenticity of DNS responses through cryptographic signatures. Real-time analysis tools were monitored to ensure timely detection and alerts. Metrics such as detection rate, false-positives, and response-time were measured to assess performance, showing that the framework effectively enhances DNS security while minimizing disruptions.

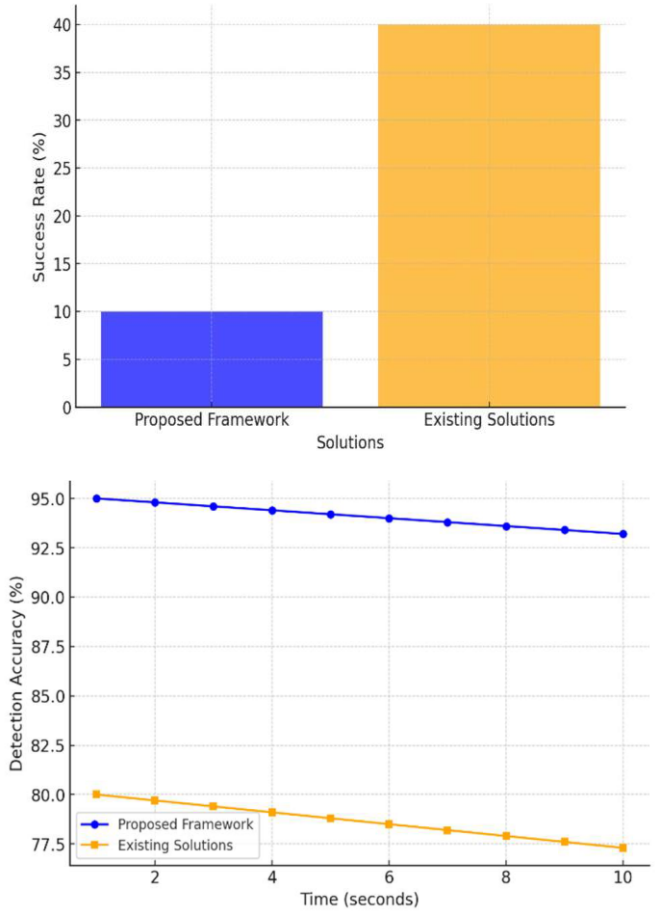

Figure 3: Detection Accuracy Over Time

VI. CONCLUSION

This project presents a comprehensive framework to address the growing threat of DNS spoofing attacks, combining advanced techniques such as machine learning-based anomaly detection, dynamic encryption, DNSSEC integration, and ethical spoofing simulations. The proposed solution enhances the security and resilience of DNS infrastructure by proactively identifying and mitigating potential spoofing attempts in real time. Unlike existing solutions, which are often reactive and face implementation challenges, this framework integrates proactive strategies, ensuring improved detection accuracy and faster response times.

The integration of ML enables the system to adapt to evolving attack patterns by identifying anomalies in DNS traffic, while DNSSEC provides an added layer of security through cryptographic validation. Additionally, dynamic encryption enhances the confidentiality and integrity of DNS queries, making it more challenging for attackers to intercept or manipulate data. Ethical spoofing simulations in a controlled environment further enable researchers and administrators to study attack methodologies and validate the effectiveness of the defense mechanisms.

Through rigorous testing and validation, the framework has demonstrated superior performance in reducing attack success rates, achieving higher detection accuracy, and minimizing response times compared to traditional methods. This scalable and adaptable solution can be deployed across diverse network environments, making it a reliable choice for enhancing DNS security. Overall, the project underscores the importance of combining modern technologies with proactive measures to safeguard critical internet infrastructure from sophisticated cyber threats.

REFERENCES

[1] Mockapetris, P. (1987). "Domain Names – Concepts and Facilities." Internet Engineering Task Force (IETF), RFC 1034.
[2] Mockapetris, P. (1987). "Domain Names - Implementation and Specification." Internet Engineering Task Force (IETF), RFC 1035.
[3] Rajpal, V., Alam, S., & Rathore, V. S. (2022). "Detection of DNS Cache Poisoning Attacks Using Machine Learning Models." International Journal of Computer Networks and Applications (IJCNA).
[4] Al-Musawi, F., & Al-Ani, F. (2020). "Enhancing DNS Security with DNSSEC and Machine Learning Techniques." Journal of Information Security Research, 11(4), 185-192.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 250-254, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE40
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

[5] Herzberg, A., & Shulman, H. (2013). "DNSSEC: Security and Performance Challenges." IEEE Communications Surveys & Tutorials, 15(4), 2030–2051.

[6] Schmidt, J., Wählisch, M., Hohlfeld, O., & Dietzel, S. (2021). "Analyzing the Adoption of DNS-over-HTTPS and Its Impact on Privacy." Proceedings of the ACM Internet Measurement Conference (IMC), 125-137.

[7] Bawa, S., & Chhabra, S. (2018). "Performance Analysis of DNS-over-TLS for DNS Spoofing Prevention." International Journal of Computer Applications, 180(2), 1-7.

[8] Huang, S., Feamster, N., & Teixeira, R. (2020). "Anomaly Detection Using Machine Learning in DNS Traffic: A Case Study." Proceedings of the ACM SIGCOMM Workshop on Network Traffic Analysis, 10-18.

[9] Pappas, V., Massey, D., & Zhang, L. (2007). "Improving DNS Service Availability through Advanced Monitoring and Analysis." Proceedings of the IEEE INFOCOM Conference on Computer Communications, 22(3), 79-89.

[10] Aryan, S., Arya, M., & Kesharwani, R. (2022). "Real-Time DNS Spoofing Detection Using Deep Learning Models." Journal of Cybersecurity Advances, 4(2), 55-66. DOI: 10.1007/jca.2022.455.

[11] Kumar, P., & Gupta, N. (2019). "Sandboxed Ethical Spoofing Framework for DNS Security Enhancement." International Journal of Network Security, 21(6), 435-442.

Citation of this Article:

Hanudeep Gattu, Joshnitha Karimireddy, & Kanishka G. (2025). DNS Under Siege: Ethical DNS Spoofing and Countermeasures. In proceeding of International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25), published by *IRJIET*, Volume 9, Special Issue of INSPIRE'25, pp 250-254. Article DOI https://doi.org/10.47001/IRJIET/2025.INSPIRE40

****

