

Enhancing Network Security Through AI-Driven DNS Filtering and Threat Intelligence Correlation

Author's :- Ashish Kurkule, Kshitij Bansod, Atharva Ganorkar

Guided By :- Prof. Pinky Jaiprakash Dembla

E-mail: @ashishkurkule@gmail.com

Abstract

In today's world, where cyber threats are becoming more advanced and frequent, protecting the Domain Name System (DNS) traffic is more important than ever. This paper introduces a smart, AI-powered DNS filtering system that works by using live threat intelligence data from different sources to catch and block harmful domains in real-time. We've used machine learning models that were trained on a wide variety of known domain data, and connected them with real-time APIs that provide updates on potential threats. This system improves the typical DNS filtering process by learning and adapting to new threats continuously, making it better at spotting new and hidden dangers on the internet.

Keywords: DNS Filtering, Threat Intelligence, Machine Learning, Network Security, Malicious Domains

INTRODUCTION :-

The Domain Name System (DNS) is a foundational component of the internet, responsible for translating human-readable domain names into IP addresses. Due to its critical role, DNS is often targeted for malicious activities such as phishing, botnet command and control (C2), and data exfiltration. Traditional DNS filtering mechanisms rely on static blacklists, which are often insufficient against zero-day threats and rapidly changing attack vectors. This research explores the fusion of AI/ML models with real-time threat intelligence to provide an adaptive and robust DNS filtering mechanism.

PROPOSED SYSTEM :-

Our system is built from four main parts: a DNS interceptor, a threat intelligence aggregator, an AI-based classification engine, and a response handler. Together, these components work to inspect DNS traffic, detect possible threats, and act quickly to block them.

- DNS Interceptor
This component checks every DNS request before it is completed. It ensures that the process doesn't slow down the network much, while still keeping it secure.
- Threat Intelligence Aggregator
This part collects data about threats from multiple sources, both free and paid, like AlienVault OTX and VirusTotal. This gives us a constantly updating list of suspicious domains and patterns.
- AI Classification Engine
Here, we use machine learning methods such as Random Forest, Support Vector Machine (SVM), or LSTM models to decide whether a domain is safe or harmful. These models look at different features of a domain like the words used in the name, information from WHOIS databases, and behavior patterns in DNS traffic.
- Response Handler
Based on what the AI model decides, this part either blocks the domain or allows it. If it's harmful, it is also logged for record-keeping and further analysis.

EXPERIMENTAL SETUP AND RESULTS :-

The system was evaluated using a dataset of 20,000 domain samples, balanced between benign and malicious labels. Features were extracted using domain parsing techniques, WHOIS records, and threat feed correlation. The Random Forest classifier yielded the highest accuracy of 96.2%.

- **3.1 Performance Metrics**

Accuracy: 96.2%

Precision: 95.8%

Recall: 96.7%

F1-Score: 96.2%

- **3.2 Threat Feed Efficacy**

Cross-verification with multiple feeds enhanced the detection rate by 8% over single-source filtering, demonstrating the importance of data correlation.

CONCLUSION:-

Our study proves that AI combined with live threat intelligence can make DNS filtering much more effective. It not only catches more threats but also adjusts itself to deal with new types of attacks. This makes it a better option than traditional methods. In the future, we want to expand this system to detect more complex threats like DNS tunneling and connect it with large-scale network security tools used by businesses.

ACKNOWLEDGEMENT:-

We would like to thank our project guide and institution for providing necessary support and infrastructure for the successful completion of this research.

REFERENCES:-

- [1] Bilge, L., & Dumitras, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. ACM CCS.
- [2] Sinha, M., et al. (2019). Domain name classification using machine learning techniques. IEEE Access.
- [3] Antonakakis, M., et al. (2017). Understanding the Mirai Botnet. USENIX Security Symposium.
- [4] OTX. AlienVault Open Threat Exchange. <https://otx.alienvault.com/>
- [5] VirusTotal. Online threat intelligence platform. <https://www.virustotal.com/>